BlackArmor® NAS 440/420
Benutzerhandbuch

BlackArmor® NAS 440/420-Benutzerhandbuch

©2010 Seagate Technology LLC. Alle Rechte vorbehalten. Seagate, Seagate Technology, das Wave-Logo und FreeAgent sind Marken oder eingetragene Marken von Seagate Technology LLC oder einer ihrer Tochtergesellschaften. Alle anderen Marken oder eingetragenen Marken sind Eigentum der jeweiligen Rechtsinhaber. Bezogen auf die Festplattenkapazität entspricht ein Gigabyte (GB) einer Milliarde Byte, ein Terabyte (TB) entspricht eintausend Milliarden Byte. Ein Teil der angegebenen Speicherkapazität wird zur Formatierung und für andere Funktionen verwendet und steht daher nicht zur Speicherung von Daten zur Verfügung. Beispiele für verschiedene Anwendungen dienen der Veranschaulichung. Die tatsächliche Menge hängt von verschiedenen Faktoren ab, wie z. B. Dateigröße, Dateiformat, Funktionen und Anwendungssoftware. Produktangebote oder Spezifikationen können ohne vorherige Ankündigung geändert werden.

Seagate Technology LLC
920 Disc Drive
Scotts Valley CA 95066 USA

Informationen zu Open-Source-Komponenten und Lizenzen

Informationen zu den Open-Source-Komponenten und Lizenzen von Seagate-Produkten finden Sie auf der Seagate-Website unter www.seagate.com/support.

Inhalt

1. Vorwort 6
Über dieses Handbuch 6
Lieferumfang 6
Systemanforderungen 7
Weitere Informationen 7

2. Übersicht über Seagate BlackArmor® NAS 440/420 8
Einführung 8
Der BlackArmor-Server 8
Hauptkomponenten des BlackArmor-Server-Pakets 9
Ausstattung des BlackArmor-Servers 9
Verwendung des BlackArmor-Servers 11
Unterschied zwischen BlackArmor-Administrator und -Benutzer 11
BlackArmor-Administratoren 11
BlackArmor-Benutzer 12
Erste Schritte 12
Erste Schritte für BlackArmor-Administratoren 12
Erste Schritte für BlackArmor-Benutzer 13

3. Installation und Einrichtung des BlackArmor®-Servers 14
Einführung 14
Installation und Einrichtung für Administratoren 15
Installieren des BlackArmor-Servers und der Software 15
Herstellen der Verbindung zum Server 16
Ersteinrichtung 17
Erstellen von Freigaben 18
Erstellen von Benutzerkonten 19
Bereitstellen der BlackArmor-Benutzerinformationen 19
Einrichten des Zugriffs auf den BlackArmor-Server über Seagate Global Access 20
Anschließen eines USB-Druckers an den BlackArmor-Server 21
Einrichten des BlackArmor-Servers als Media Server 22
Nächste Schritte für Administratoren 23
Erste Schritte für BlackArmor-Benutzer 24
Optionale Schritte 25
Erstellen eines Seagate Global Access-Kontos 26

4. Optimale Nutzung des BlackArmor®-Servers 27

Einführung 27

Die Rolle des BlackArmor-Administrators 28

Standardeinstellungen des BlackArmor-Servers 29

Verwalten von Datenträgern, Freigaben und Speicher des BlackArmor-Servers 30

- Übersicht über Datenträger und Freigaben 30
- Verwalten von Datenträgern 31
- Verwalten von Freigaben 33
- Festlegen von Speicherplatzbegrenzungen für BlackArmor-Benutzer 35
- Festlegen von Kulanzzeiten für Kontingente 35
- Steuerung von Downloads aus dem Internet auf den BlackArmor-Server 35

Verwalten von BlackArmor-Benutzern 36

- Verwalten von Benutzerkonten 36
- Erstellen und Bearbeiten von Benutzergruppen 37

Netzwerksicherung der Dateien auf dem BlackArmor-Server 37

Einrichten der Link Aggregation 39

Einrichten des BlackArmor-Servers als Media Server 39

Überwachen des BlackArmor-Servers 39

- Überwachen des Status anhand der LCD-Anzeige des Servers 40
- Überwachen des Status anhand der LED-Anzeigen des Servers 40
- Verwenden von E-Mail-Benachrichtigungen über den Serverstatus . . . 41
- Überprüfen des Festplattenstatus mit SMART 41

Ändern der erweiterten Einstellungen des BlackArmor-Servers 42

- DDNS-Einstellungen 42
- Dateiprotokolleinstellungen 42
- NTP-Einstellungen 43
- Energiespareinstellungen 43
- SSL-Einstellungen 43
- USV-Einstellungen 43
- Internet-Protokoll-Einstellungen 44
- Arbeitsgruppen- und Domäneneinstellungen 44

Warten des BlackArmor-Servers 45

- Hinweise zu Sicherheit und Wartung der Hardware 45
- Aktualisieren der Server-Firmware 46

Zurücksetzen des BlackArmor-Servers 46

5. Tipps für BlackArmor®-Benutzer 47
Einführung 47
Informationen zum BlackArmor-Benutzerkonto 47
Zugriffseinschränkungen 47
Speicherplatzeinschränkungen 48
Automatische Sortierung von Mediendateien 49
Kulanzzeiten für Kontingente 49
Unterstützung für Dateiprotokolle 49
Zugreifen auf Freigaben und Dateien auf dem BlackArmor-Server 49
Sichern von Dateien 50
Sichern von Dateien mit BlackArmor Backup 50
Sichern von Server zu Server 50
Sichern von oder auf externe USB-Laufwerke 51
Zugreifen auf BlackArmor-Dateien über das Internet 51
Herunterladen großer Dateien aus dem Internet auf den BlackArmor-Server 52
Wiederherstellen gelöschter Dateien im Papierkorb 52

6. Beheben von Problemen 53
Allgemeine Tipps zur Problembehebung 53
Häufige Probleme und Lösungen 53
Die Verbindung zum Server über das lokale Netzwerk kann nicht hergestellt werden. 53
Die Verbindung zum Server über das Internet kann nicht hergestellt werden. 54
BlackArmor Manager kann nicht geöffnet werden. 54
Die Anmeldung bei BlackArmor Manager funktioniert nicht. 54
Auf eine Freigabe kann nicht zugegriffen werden. 54
Auf eine Datei in einer Freigabe kann nicht zugegriffen werden. 54
In einer Freigabe können keine Dateien mehr gespeichert werden, weil der Datenträger voll ist. 54
Die Firmware-Aktualisierung konnte nicht durchgeführt werden. 55
Das Streaming von Musik vom BlackArmor-Server funktioniert nicht. 55
Ein Datenträger befindet sich im eingeschränkten Betrieb. 55
Austauschen von Festplatten 55
WARNUNG: Vorsichtsmaßnahmen gegen elektrostatische Entladung . . . 55
Entfernen einer Festplatte 55
Austauschen einer Festplatte 57

7. Technische Daten 59

8. Glossar 60

1. Vorwort

- Über dieses Handbuch
- Lieferumfang
- Systemanforderungen
- Weitere Informationen

Über dieses Handbuch

In diesem *Benutzerhandbuch* finden Sie alle Informationen, die Sie benötigen, um den Seagate BlackArmor® NAS 440/420 (BlackArmor-Server) einzurichten und zu nutzen.

Das Handbuch enthält vollständige Anleitungen zur Einrichtung des BlackArmor-Servers sowie Informationen über seine Komponenten und Funktionen. Außerdem gibt es einen Überblick darüber, wie Sie den BlackArmor-Server optimal nutzen können, um wachsende und veränderliche Anforderungen zu erfüllen.

Hinweis: Schrittweise Anleitungen zur Verwendung der BlackArmor-Softwaretools finden Sie in der Onlinehilfe der jeweiligen Software.

Einige Themen in diesem Handbuch sind nur für BlackArmor-*Administratoren* – Benutzer mit Zugang zu den Verwaltungsfunktionen des BlackArmor-Servers – relevant. Informationen nur für Administratoren sind deutlich als solche gekennzeichnet.

Lieferumfang

Zum Lieferumfang des BlackArmor-Servers gehören:

- BlackArmor-Server
- Netzteil
- Ethernetkabel
- Installations-CD mit Software, Dokumentation und Garantieinformationen
- *BlackArmor-Schnellstartanleitung*

Systemanforderungen

Alle Computer, die zum Zugriff auf den BlackArmor-Server verwendet werden sollen, müssen die folgenden Anforderungen erfüllen:

- Microsoft Windows®- oder Apple Macintosh®-Computer mit einem der folgenden Betriebssysteme:
  - Windows XP oder Windows Vista® mit dem jüngsten Service Pack
  - Mac OS X ab 10.4.11
- Netzwerkkarte
- Unterstützte Webbrowser:
  - Microsoft Internet Explorer 6, 7 oder 8 (nur Windows)
  - Apple Safari 3, 4 oder höher (Windows oder Mac)
  - Mozilla Firefox 2, 3 oder höher (Windows oder Mac)

Zusätzlich sind erforderlich:

- Lokales Netzwerk (LAN oder WLAN)
- Netzwerk-Switch oder -Router mit mindestens einem freien Ethernetanschluss
- Internetverbindung (für Fernzugriff auf den Server sowie Software- und Firmware-Aktualisierungen)

Weitere Informationen

Weitere Informationen über den BlackArmor-Server:

- BlackArmor-Schnellstartanleitung (gedruckt)
- BlackArmor Manager-Hilfe
- BlackArmor Discovery-Hilfe
- BlackArmor Backup-Benutzerhandbuch
- BlackArmor Backup-Hilfe
- Readme-Datei

Weitere Informationen finden Sie auf der Seagate-Website unter www.seagate.com.

2. Übersicht über Seagate BlackArmor® NAS 440/420

- Einführung
- Der BlackArmor-Server
- Verwendung des BlackArmor-Servers
- Unterschied zwischen BlackArmor-Administrator und -Benutzer
- Erste Schritte

Einführung

Dieses Kapitel stellt die Komponenten und Ausstattung des BlackArmor® NAS 440/420 (BlackArmor-Server) vor, beschreibt, wozu der BlackArmor-Server genutzt werden kann und erklärt den Unterschied zwischen BlackArmor-Administratoren und normalen BlackArmor-Benutzern.

Außerdem finden Sie hier Hinweise zur Einrichtung und optimalen Nutzung des BlackArmor-Servers. (Zum Unterschied zwischen Administratoren und Benutzern siehe „Unterschied zwischen BlackArmor-Administrator und -Benutzer“ auf Seite 11.)

Der BlackArmor-Server

Der BlackArmor-Server ist ein Dateiserver – ein Gerät, das verwendet wird, um verschiedene Arten von Dateien zu speichern und den Benutzern in einem lokalen Netzwerk zur Verfügung zu stellen. Der BlackArmor-Server verfügt über vier SATA-Festplatten und bietet integrierte Datensicherheit, um Ihre Daten gegen Festplattenausfälle und andere Katastrophen zu schützen.

Der BlackArmor-Server wird mit Software ausgeliefert, die Sie dabei unterstützt, Ihre Dateien zu sichern, zu speichern, freizugeben und zu schützen.

Der BlackArmor-Server wird vor allem in Kleinunternehmen und Heimbüros eingesetzt, um wichtige Dateien wie Kundendateien, Geschäftsunterlagen, Finanzinformationen usw. zu speichern, zu schützen und im lokalen Netzwerk oder über das Internet für andere verfügbar zu machen.

Hauptkomponenten des BlackArmor-Server-Pakets

Das BlackArmor-Server-Paket besteht aus vier Hauptkomponenten:

- **BlackArmor-Server**: Die Hardware mit den Festplatten, die Ihre Dateien speichern und schützen.
- **BlackArmor Discovery**: Software, die den BlackArmor-Server im Netzwerk findet und mit Ihrem Computer verbindet.
- **BlackArmor Manager**: Ein in den Server integriertes Tool, mit dem Sie den BlackArmor-Server über einen Webbrowser von Ihrem Computer aus (oder sogar per Fernzugriff) einrichten, ändern und überwachen können.
- **BlackArmor Backup**: Software, mit der Sie Dateien, Anwendungen und sogar Betriebssysteme auf den BlackArmor-Server sichern können. Außerdem können Sie mit dieser Software Ihr System und Ihre Daten wiederherstellen. Weitere Informationen finden Sie im *BlackArmor Backup-Benutzerhandbuch*.

Ausstattung des BlackArmor-Servers

Hinweis: Die in diesem Abschnitt beschriebenen Elemente sind in den Abbildungen auf Seite 10 dargestellt.

Die Ausstattung des BlackArmor-Servers umfasst:

- Vier SATA-Festplatten (Serial ATA), die *Hot-Swap-fähig* (leicht austauschbar) sind. Die Festplatten befinden sich hinter der Serverklappe.
- Zwei Ethernet- oder *LAN*-Anschlüsse, die den Zugriff auf den Server über das lokale Netzwerk oder das Internet ermöglichen.

Die beiden LAN-Anschlüsse des Servers können für *Link Aggregation* konfiguriert werden. Dabei werden beide LAN-Anschlüsse gleichzeitig für die Verbindung zum Netzwerk verwendet. Dies ermöglicht einen sogenannten Failover-Schutz, d. h., die zweite Verbindung (Port) übernimmt, wenn die erste ausfällt. Siehe Seite 39.

Sie können auch einen LAN-Anschluss für die Verbindung zum Netzwerk verwenden und den anderen für die Archivsicherung, bei der eine genaue Kopie der Daten des BlackArmor-Servers auf einem zweiten BlackArmor-Server erstellt und laufend fortgeführt wird. Siehe Seite 37.

- Vier USB-Anschlüsse, an die Sie ein externes USB-Laufwerk zur direkten Datensicherung vom und auf den Server, eine unterbrechungsfreie Stromversorgung (USV) oder einen USB-Drucker anschließen können, der allen Benutzern im lokalen Netzwerk zur Verfügung steht.
- LED-Anzeigen, die Aktivität und Status von Anschlüssen, Festplatten und Server anzeigen. Siehe Seite 41.
- Eine LCD-Anzeige, die die aktuellen Servereinstellungen und Statusinformationen zeigt und auf der Meldungen über *Ereignisse* (Probleme oder Einstellungsänderungen) auf dem Server ausgegeben werden. Mit Tasten neben der Anzeige können Sie die verfügbaren Informationen abrufen. Siehe Seite 40.

Wenn die LEDs eine Änderung an Einstellungen oder Status anzeigen, erscheinen Informationen über die Änderung auf der LCD-Anzeige.

- Eine Reset-Taste, mit der Sie Benutzername und Kennwort für den BlackArmor-Server auf die Standardeinstellungen zurücksetzen können.

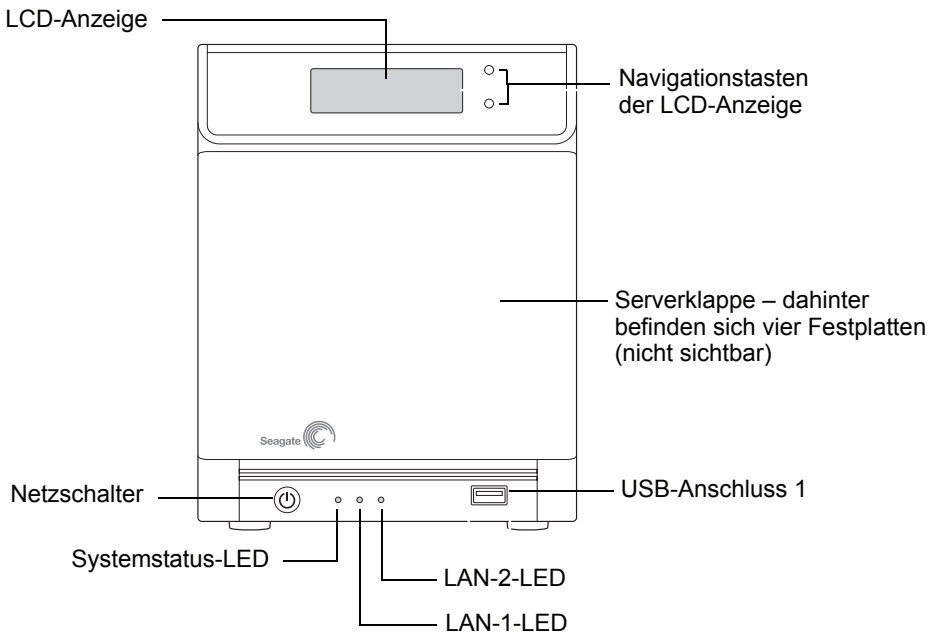


Abbildung 1: Vorderseite des BlackArmor-Servers

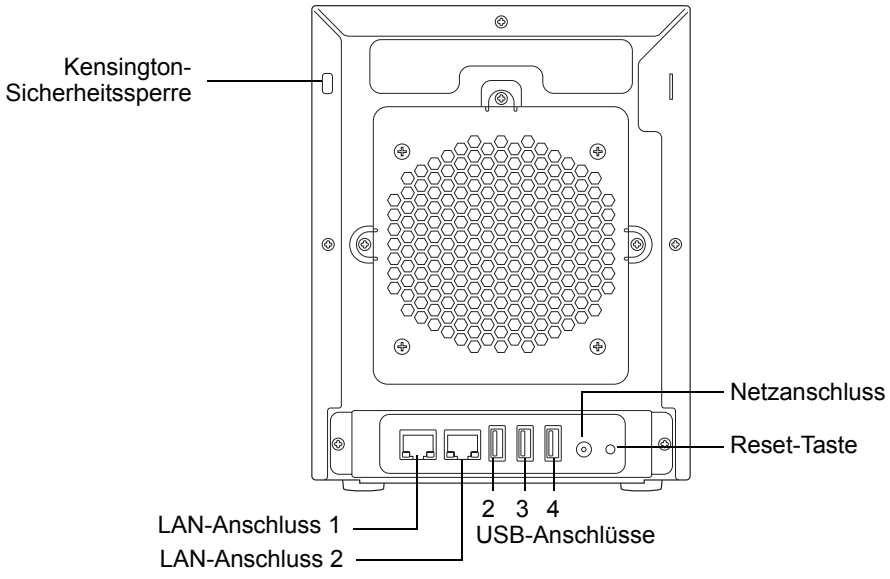


Abbildung 2: Rückseite des BlackArmor-Servers

Verwendung des BlackArmor-Servers

Der BlackArmor-Server bietet vielfältige Einsatzmöglichkeiten:

- Sie können einen zentralen Speicherort für Dateien einrichten, die Sie über das lokale Netzwerk oder das Internet für andere Benutzer verfügbar machen wollen.
- Sie können automatisch Sicherungskopien aller Ihrer Dateien – selbst von Betriebssystemen – erstellen und fortschreiben lassen.
- Sie können Dateien wie etwa Verträge, Präsentationen und Berichte über das lokale Netzwerk oder das Internet für Kollegen oder Geschäftskunden verfügbar machen.
- Sie können nach einer Katastrophe – versehentliches Löschen wichtiger Dateien, Festplattenausfall, Diebstahl des Computers usw. – Ihre Daten rasch wiederherstellen und weiterarbeiten.
- Sie können von jedem Ort der Welt über das Internet auf den BlackArmor-Server zugreifen, um Dateien herunterzuladen oder Dateien hochzuladen, die Sie sicher speichern oder für andere verfügbar machen möchten, während Sie unterwegs sind.
- Sie können einen USB-Drucker für andere Benutzer im lokalen Netzwerk verfügbar machen.
- Sie können einen Media Server einrichten, sodass alle Benutzer im lokalen Netzwerk heruntergeladene Fotos, Videos und Musik genießen können.
- Sie können den iTunes®-Dienst auf dem Server einrichten, um den Benutzern das Streaming von Musik zu Netzwerkcomputern mit iTunes zu ermöglichen.

Unterschied zwischen BlackArmor-Administrator und -Benutzer

Neben den von allen nutzbaren Funktionen wie der Dateifreigabe hat der BlackArmor-Server auch Verwaltungsfunktionen, die nur von einer oder zwei Personen – in diesem Handbuch als BlackArmor-*Administratoren* bezeichnet – verwendet werden sollten.

In diesem Handbuch werden alle Personen, die auf den BlackArmor-Server zugreifen, als BlackArmor-*Benutzer* bezeichnet.

BlackArmor-Administratoren

BlackArmor-Administratoren haben vollen Zugriff auf alle Funktionen und Einstellungen des BlackArmor-Servers und alle darauf gespeicherten Dateien. BlackArmor-Administratoren können folgende Aufgaben ausführen:

- Ändern aller Servereinstellungen
- Erstellen und Bearbeiten von Benutzerkonten und Gruppenkonten
- Einrichten und Bearbeiten von Ordnern (oder *Freigaben*)

- Aktualisieren der Server-Firmware
- Austauschen defekter Festplatten
- Zurücksetzen von Servername und -kennwort auf die Standardeinstellungen

BlackArmor-Benutzer

Alle BlackArmor-Benutzer, einschließlich der Administratoren, können folgende Funktionen nutzen:

- Ändern ihres Anmeldekennworts
- Speichern und Freigeben von Dateien auf dem BlackArmor-Server
- Sichern von Dateien auf den BlackArmor-Server
- Zugriff auf den BlackArmor-Server über das Internet durch Seagate Global Access
- Herunterladen großer Dateien aus dem Internet direkt auf den BlackArmor-Server
- Zugriff auf Musik, Videos und Fotos (wenn der BlackArmor-Server als Media Server eingerichtet ist)
- Verfügbarmachen eines an den BlackArmor-Server angeschlossenen USB-Druckers für andere Benutzer

Hinweis: Der Administrator kann auch Benutzerkonten mit Administratorrechten erstellen. Weitere Informationen finden Sie in der Hilfe von BlackArmor Manager.

Erste Schritte

Dieser Abschnitt beschreibt die ersten Aufgaben für BlackArmor-Administratoren und -Benutzer.

Erste Schritte für BlackArmor-Administratoren

Erste Aufgaben für die Nutzung des BlackArmor-Servers:

1. Installieren Sie den BlackArmor-Server und die Software (siehe Seite 15).
2. Stellen Sie mit BlackArmor Discovery eine Verbindung zum Server her (siehe Seite 16).
3. Führen Sie mit BlackArmor Manager die Ersteinrichtung des Servers durch (siehe Seite 17).
4. Erstellen Sie eigene Ordner (oder Freigaben) für die Speicherung von Dateien (siehe Seite 18).
5. Erstellen Sie Benutzerkonten für alle, die auf den BlackArmor-Server zugreifen sollen, und weisen Sie den einzelnen Benutzern die gewünschten Zugriffsberechtigungen für die erstellten Freigaben zu (siehe Seite 19).
6. Geben Sie allen BlackArmor-Benutzern die entsprechenden Benutzerkontoinformationen (siehe Seite 19).

7. *(Optional)* Aktivieren Sie Global Access in BlackArmor Manager, um den Zugriff auf den BlackArmor-Server über das Internet zu ermöglichen (siehe Seite 20).
8. *(Optional)* Schließen Sie einen USB-Drucker an den BlackArmor-Server an, um ihn für alle Benutzer im lokalen Netzwerk verfügbar zu machen (siehe Seite 21).
9. *(Optional)* Schließen Sie eine unterbrechungsfreie Stromversorgung an den BlackArmor-Server an, um bei Stromausfällen die Versorgung aufrechtzuerhalten (siehe Seite 43).
10. *(Optional)* Richten Sie den BlackArmor-Server als Media Server ein, sodass BlackArmor-Benutzer auf Musik, Fotos und Videos zugreifen können (siehe Seite 22).
11. Fahren Sie mit dem nächsten Abschnitt Erste Schritte für BlackArmor-Benutzer fort, um mit der Nutzung des BlackArmor-Servers zum Speichern, Sichern und Freigeben Ihrer eigenen Dateien zu beginnen.

Erste Schritte für BlackArmor-Benutzer

Erste Aufgaben für die Nutzung des BlackArmor-Servers:

1. Vergewissern Sie sich, dass Sie Folgendes vom BlackArmor-Administrator erhalten haben:

- BlackArmor Discovery-Software
- BlackArmor Backup-Software
- BlackArmor-Benutzername und -Kennwort
- Namen der Freigaben, auf die Sie zugreifen können
- Angaben zu etwaigen Zugriffseinschränkungen (z. B. nur Lesezugriff auf eine bestimmte Freigabe)
- BlackArmor NAS 440/420-Benutzerhandbuch

2. Installieren Sie die BlackArmor-Software (siehe Seite 15).

Falls Sie bereits ein anderes Programm für die regelmäßige Dateisicherung verwenden, brauchen Sie BlackArmor Backup nicht zu installieren.

3. Stellen Sie mit BlackArmor Discovery eine Verbindung zum Server und zu den Freigaben her, auf die Sie Zugriff haben (siehe Seite 16).
4. Machen Sie Ihre Dateien verfügbar, indem Sie sie in Freigaben speichern, auf die andere Benutzer über das lokale Netzwerk oder das Internet zugreifen können.
5. *(Optional)* Erstellen Sie eine vollständige Sicherung Ihrer wichtigen Dateien oder richten Sie regelmäßige Sicherungen ein. Verwenden Sie dazu BlackArmor Backup (siehe Seite 50).
6. *(Optional)* Falls ein USB-Drucker an den BlackArmor-Server angeschlossen ist, fügen Sie diesen gemäß den Anweisungen für Ihr Betriebssystem zur Liste der verfügbaren Drucker hinzu.

3. Installation und Einrichtung des BlackArmor®-Servers

- Einführung
- Installation und Einrichtung für Administratoren
- Erste Schritte für BlackArmor-Benutzer

Einführung

In diesem Kapitel finden Sie Schritt-für-Schritt-Anleitungen für die Installation und Einrichtung des BlackArmor®-Servers und der Software.

Falls Sie kein BlackArmor-Administrator sind, gehen Sie zu Seite 24.

Hinweis: Eine Übersicht über die Einrichtungsschritte finden Sie unter „Erste Schritte“ auf Seite 12.

Die folgende Abbildung zeigt eine typische BlackArmor-Server und -Software-Installation.

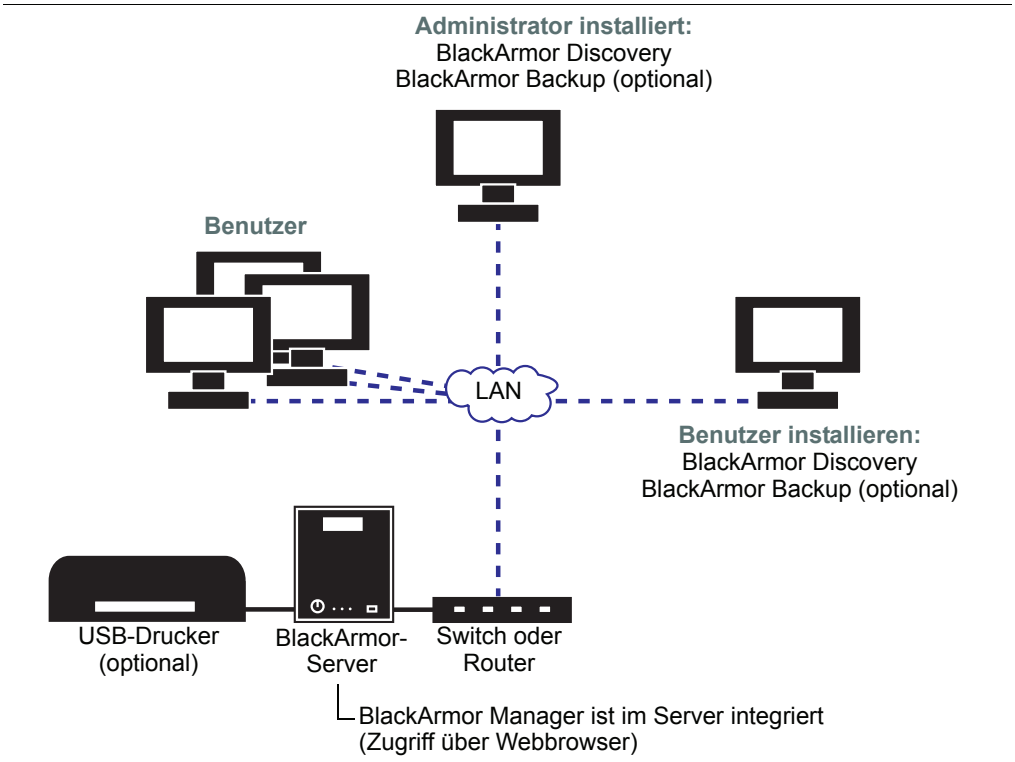


Abbildung 3: Typische BlackArmor-Installation

Installation und Einrichtung für Administratoren

Falls Sie kein BlackArmor-Administrator sind, gehen Sie zu Seite 24.

Installieren des BlackArmor-Servers und der Software

Vor der Installation:

- Vergewissern Sie sich, dass Ihr Computer den Systemanforderungen auf Seite 7 entspricht.
- Achten Sie darauf, dass der Server auf einer stabilen und ebenen Oberfläche steht und eine ausreichende Belüftung gewährleistet ist. Die Belüftungsschlitze des Servers dürfen nicht blockiert sein und der Server darf nicht in der Nähe einer Wärmequelle aufgestellt werden. Achten Sie darauf, den Server nicht an einem Standort aufzustellen, an dem die Gefahr besteht, dass Flüssigkeiten auf das Gerät verschüttet werden.
- Falls Ihnen das Anheben mäßig schwerer Objekte Schwierigkeiten bereitet, besorgen Sie sich Hilfe, um den Server zu bewegen.

So installieren Sie den BlackArmor-Server und die Software:

1. Schließen Sie den BlackArmor-Server mit dem mitgelieferten Ethernetkabel an einen Switch oder Router im lokalen Netzwerk an. Schließen Sie das Ethernetkabel an den Anschluss 1 an, wie in der Abbildung dargestellt.

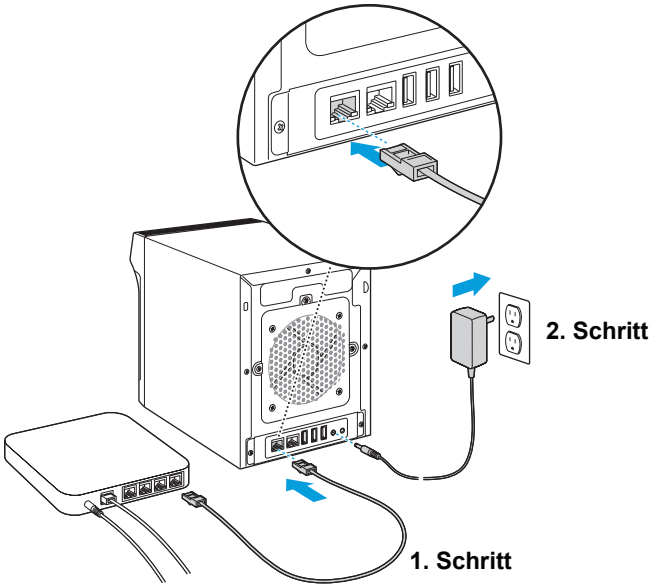


Abbildung 4: Anschließen von Strom- und Netzwerkkabeln

Falls Sie ein zweites Ethernetkabel haben und beide LAN-Anschlüsse an den Switch oder Router anschließen möchten, schließen Sie das Kabel jetzt an. Weitere Informationen finden Sie auf Seite 39.

2. Schließen Sie den BlackArmor-Server mit dem mitgelieferten Netzteil an eine geerdete Steckdose an.

Der Server schaltet sich automatisch ein und die LEDs an der Vorderseite des Servers beginnen zu leuchten. Die LCD-Anzeige zeigt den Startvorgang an.

3. Legen Sie die Installations-CD-ROM in Ihren Computer ein.

Der Installationsassistent wird automatisch gestartet. Installieren Sie BlackArmor Discovery *und* BlackArmor Backup, falls Sie nicht bereits eine andere Sicherungssoftware verwenden.

4. Klicken Sie auf **Weiter**.
5. Klicken Sie auf **Weiter**, wenn Sie das Standardverzeichnis für die Installation übernehmen möchten, oder klicken Sie auf **Durchsuchen** und wählen Sie ein anderes Verzeichnis aus. Klicken Sie anschließend auf **Weiter**.
6. Klicken Sie auf **Weiter**, wenn Sie die Standardbezeichnung für den Programmordner übernehmen möchten, oder geben Sie einen anderen Namen ein und klicken Sie dann auf **Weiter**.

BlackArmor Discovery wird installiert.

7. Klicken Sie auf **Fertig stellen**.

Herstellen der Verbindung zum Server

So stellen Sie eine Verbindung zum BlackArmor-Server her:

1. Doppelklicken Sie auf das BlackArmor Discovery-Symbol auf dem Desktop (Windows) oder im Ordner „Anwendungen“ (Mac).

Beim Start sucht BlackArmor Discovery automatisch nach BlackArmor-Servern im lokalen Netzwerk und zeigt diese in einer Liste an.

2. Wählen Sie den neuen BlackArmor-Server aus.
3. (Windows) Klicken Sie auf **Laufwerkinfos anzeigen** und dann auf **Verwalten**.
   (Mac) Klicken Sie auf **Server verwalten**.

BlackArmor Manager wird geöffnet.

Hinweis: BlackArmor Discovery bleibt geöffnet, bis Sie es schließen. Sie können das Programm jederzeit durch einen Doppelklick auf das Discovery-Symbol auf dem Desktop (Windows) oder im Ordner „Anwendungen“ (Mac) wieder öffnen.

4. Melden Sie sich mit den Standardzugangsdaten an. (Beachten Sie bei Benutzername und Kennwort die Groß-/Kleinschreibung.)

Benutzername: **admin**

Kennwort: **admin**

Hinweis: Die Standardeinstellungen des BlackArmor-Servers ermöglichen es Ihnen, sofort mit dem Speichern, Freigeben und Sichern von Dateien zu beginnen. Weitere Informationen finden Sie auf Seite 29.

Ersteinrichtung

Wenn Sie sich zum ersten Mal beim BlackArmor-Server anmelden, wird der Einrichtungsassistent aufgerufen. So führen Sie die Ersteinrichtung aus:

1. Klicken Sie auf **Weiter**, um mit der die Ersteinrichtung des BlackArmor-Servers zu beginnen.
2. Lesen Sie die Lizenzvereinbarung für Seagate BlackArmor und klicken Sie dann auf **Zustimmen**.
3. Passen Sie die Grundeinstellungen des Servers an:

- Geben Sie einen Namen für den BlackArmor-Server ein. Verwenden Sie eine eindeutige, aussagekräftige Bezeichnung, damit der Server im lokalen Netzwerk leicht zu erkennen ist. Der Name kann aus bis zu 16 alphanumerischen Zeichen bestehen und darf auch Bindestriche enthalten. Leerzeichen dürfen nicht verwendet werden.
- Geben Sie eine Beschreibung für den Server ein, anhand derer Sie ihn von anderen Servern im lokalen Netzwerk unterscheiden können (z. B. Angaben zu Standort, Art der Daten oder anderen Merkmalen).

4. Wählen Sie die entsprechende Zeitzone für den Standort des Servers aus und stellen Sie Datum und Uhrzeit ein.
5. Klicken Sie auf **Weiter**.
6. Geben Sie ein neues Administratorkennwort ein, bestätigen Sie es und klicken Sie dann auf **Weiter**.

Seagate empfiehlt dringend, das Administratorkennwort zu ändern, um den BlackArmor-Server und die darauf gespeicherten Daten zu schützen. Kennwörter können aus bis zu 16 alphanumerischen Zeichen bestehen. Dabei wird die Groß-/Kleinschreibung berücksichtigt.

Beispiel für ein gutes Kennwort: **LEag29ue**

Beispiel für ein schlechtes Kennwort: **blackarmor**

7. Wählen Sie den gewünschten Netzwerkmodus aus und klicken Sie auf **Weiter**.

Standardmäßig ist beim BlackArmor-Server der Netzwerkmodus DHCP eingestellt.

Falls Sie nicht in einem Großunternehmen mit eigener IT-Abteilung arbeiten, empfiehlt Seagate, den DHCP-Netzwerkmodus zu verwenden.

8. Klicken Sie auf **Weiter**, um die Einrichtung abzuschließen.
9. Überprüfen Sie die Zusammenfassung der Einstellungen. Klicken Sie auf **Zurück**, um Änderungen vorzunehmen, oder klicken Sie auf **Fertig stellen**, um die Einrichtung abzuschließen.

Erstellen von Freigaben

Standardmäßig sind auf dem BlackArmor-Server zwei Freigaben eingerichtet: Download und Öffentlich. Falls dies für Ihre derzeitigen Bedürfnisse ausreicht, gehen Sie zu „Erstellen von Benutzerkonten“ auf Seite 19.

Sie können auch mit der Web-Oberfläche von BlackArmor Manager eigene Freigaben erstellen, etwa um Dateien nach Kategorie (z. B. Kunden-, Projekt- und Buchhaltungsdateien) oder Abteilung (z. B. Marketing, Buchhaltung und Vertrieb) zu speichern.

So erstellen Sie eigene Freigaben:

1. Klicken Sie in der Menüleiste auf **Speicher** und dann auf **Freigaben**. Anschließend klicken Sie auf das Symbol **Hinzufügen**.
2. Geben Sie einen Namen für die neue Freigabe ein.

Verwenden Sie eine aussagekräftige Bezeichnung, damit die Freigabe auf dem Server leicht zu erkennen ist.

3. Geben Sie eine Beschreibung der Freigabe ein.
4. Wählen Sie in der Dropdownliste der Benutzerkonten den Eigentümer der Freigabe aus. (Zur Erstellung von Benutzerkonten siehe Erstellen von Benutzerkonten.)
5. Wählen Sie die Protokolle aus, die die Freigabe unterstützen soll (siehe Seite 34).
6. Falls mehrere Datenträger vorhanden sind, wählen Sie den Datenträger aus, auf dem die Freigabe erstellt werden soll.
7. Sie können die Dateien in der Freigabe gegen versehentliches Löschen schützen, indem Sie einen Papierkorb einrichten. Gelöschte Dateien im Papierkorb können bei Bedarf wiederhergestellt werden.

Klicken Sie neben **Papierkorb-Dienst** auf **Aktivieren**, um einen Papierkorb einzurichten.

8. Sie können festlegen, dass bestimmte Dateitypen in Standardordner der Freigabe heruntergeladen werden – zum Beispiel alle Musikdateien in den Ordner „Musik“.

Klicken Sie neben **Drag&Sort-Dienst** auf **Aktivieren**, um heruntergeladene Dateien automatisch sortieren zu lassen. Informationen zu diesem Dienst finden Sie unter „Besondere Funktionen für Freigaben“ auf Seite 34.

9. Sie können den BlackArmor-Server nutzen, um digitale Fotos, Videos und Musik für Benutzer im lokalen Netzwerk verfügbar zu machen. Klicken Sie neben **Mediendienst** auf **Aktivieren**, um diesen Dienst einzurichten.
10. Aktivieren Sie das Kontrollkästchen **Freigabezugriff**, um die Seite anzuzeigen, auf der Sie den Benutzer- und Gruppenzugriff für die neue Freigabe einrichten und bearbeiten können. Weitere Informationen finden Sie in der Onlinehilfe von BlackArmor Manager.
11. Klicken Sie auf **Senden**.

Die Freigabe wird erstellt.

Erstellen von Benutzerkonten

Standardmäßig ist auf dem BlackArmor-Server nur ein Administratorkonto eingerichtet. Ihre nächste Aufgabe ist daher, mit BlackArmor Manager Benutzerkonten zu erstellen.

Zur Erstellung von Benutzerkonten gehört auch, den einzelnen Benutzern Zugriff auf die Standardfreigaben oder die neu erstellten Freigaben zu geben.

So erstellen Sie ein Benutzerkonto:

1. Klicken Sie in der Menüleiste auf **Zugriff** und dann auf **Benutzer**.
2. Klicken Sie auf das Symbol **Hinzufügen**.
3. Nehmen Sie die gewünschten Einstellungen vor.

- **Benutzername**: Name, mit dem sich der Benutzer anmeldet.
- **Administratorrechte**: Macht den Benutzer zum BlackArmor-Administrator.
- **Vollständiger Name**: Der Name des Benutzers.
- **Kennwort** und **Kennwort bestätigen**: Bis zu 15 alphanumerische Zeichen, die der Benutzer beim Anmelden eingeben muss.
- **Gruppe**: Benutzergruppe, zu der das Konto gehören soll.
- **Private Benutzerfreigabe erstellen**: Legt fest, ob BlackArmor Manager eine neue private Freigabe für das Konto erstellen soll.
- **Datenträger**: Legt fest, auf welchem Datenträger (falls mehrere vorhanden sind) die private Freigabe erstellt werden soll.
- **Dienste**: Legt fest, welche Arten von Dateidienst für die private Freigabe verfügbar sein sollen.

4. Klicken Sie auf **Senden**.

Das neue Konto erscheint in der Liste der Benutzerkonten.

Hinweis: Durch die Einteilung von Benutzern in Gruppen lässt sich der Zugriff auf Freigaben schneller und einfacher verwalten. Mit Benutzergruppen können Sie den Zugriff auf Freigaben für einzelne Benutzer oder ganze Gruppen in einem Fenster bearbeiten. Weitere Informationen finden Sie auf Seite 37.

Bereitstellen der BlackArmor-Benutzerinformationen

Nach der Erstellung der Benutzerkonten versorgen Sie alle BlackArmor-Benutzer mit Folgendem, damit sie den BlackArmor-Server nutzen können:

- BlackArmor Discovery-Software
- BlackArmor Backup-Software (optional)
- BlackArmor-Benutzername und -Kennwort

- Namen der Freigaben, auf die die Benutzer Zugriff haben, sowie Angaben zu etwaigen Zugriffseinschränkungen (z. B. Lesezugriff)
- Dieses Handbuch und Angaben zu dem Abschnitt, mit dem BlackArmor-Benutzer beginnen sollten („Erste Schritte für BlackArmor-Benutzer“ auf Seite 13).

Sie können für jeden BlackArmor-Benutzer eine Kopie der Software auf der mitgelieferten CD erstellen oder die benötigte Software von www.seagate.com/support herunterladen.

Einrichten des Zugriffs auf den BlackArmor-Server über Seagate Global Access

Hinweis: Dies ist ein optionaler Schritt. Global Access kann nur von BlackArmor-Administratoren aktiviert werden.

Durch die Aktivierung von Global Access in BlackArmor Manager können Sie den Zugriff auf die Dateien und Ordner auf dem BlackArmor-Server über das Internet ermöglichen.

Seagate Global Access ist ein Service, über den Sie die Dateien auf dem BlackArmor-Server von jedem Ort aus anzeigen, herunterladen, freigeben und bearbeiten können. Sie können Seagate Global Access auch nutzen, um Dateien auf den BlackArmor-Server hochzuladen.

Damit Sie über das Internet auf den BlackArmor-Server zugreifen können, müssen folgende Voraussetzungen erfüllt sein:

- Der Administrator muss Global Access in BlackArmor Manager aktiviert haben. Dies ermöglicht den Fernzugriff auf den Server.
- Zur Nutzung dieser Funktion benötigen Sie ein Global Access-Konto. Dies gilt auch für Administratoren. Jeder Benutzer, der über das Internet auf den BlackArmor-Server zugreifen möchte, braucht ein eigenes Global Access-Konto. (Das Konto ist kostenlos.)

Aktivieren von Global Access für den Server (vom Administrator auszuführen)

1. Klicken Sie in der Menüleiste auf **Zugriff** und dann auf **Global Access**.
2. Aktivieren Sie das Kontrollkästchen **Aktivieren**.
3. Klicken Sie auf **Senden**.

Der Zugriff auf den Server wird aktiviert. Die Benutzer müssen noch ein Seagate Global Access-Konto erstellen und Global Access aktivieren, um über das Internet auf die Serverdateien zugreifen zu können. Siehe „Erstellen eines Seagate Global Access-Kontos“ auf Seite 26.

Aktivieren von Global Access als Benutzer

Nachdem der Administrator Global Access für den Server aktiviert hat, müssen auch die einzelnen Benutzer den Zugriff für ihr Benutzerkonto aktivieren.

Zur Aktivierung von Global Access benötigen Sie ein Seagate Global Access-Konto. Sie können wie unten beschrieben auf der Global Access-Seite ein Konto einrichten. Eine ausführliche Anleitung finden Sie unter „Erstellen eines Seagate Global Access-Kontos“ auf Seite 26.

1. Melden Sie sich unter Ihrem BlackArmor-Benutzerkonto beim Server an.
2. Klicken Sie in der Menüleiste auf **Global Access**. (Falls Ihr Benutzerkonto mit Administratorrechten ausgestattet ist, wählen Sie **Zugriff** und klicken Sie auf **Global Access**.)
3. Aktivieren Sie das Kontrollkästchen **Aktivieren**.
4. Falls Sie noch kein Global Access-Konto erstellt haben, klicken Sie auf **Konto erstellen**, andernfalls gehen Sie zu Schritt 5.

Ein neues Browserfenster wird geöffnet. Folgen Sie den Online-Anweisungen, um ein neues Konto zu erstellen.

5. Geben Sie die E-Mail-Adresse und das Kennwort für Ihr Seagate Global Access-Konto ein.
6. Klicken Sie auf **Senden**.

Einzelheiten dazu, wie Sie anderen Personen Zugriff auf Ihre private Freigabe geben können, finden Sie in der Dokumentation zu Global Access.

Anmelden bei Seagate Global Access

1. Melden Sie sich unter Ihrem Benutzerkonto beim Server an.
2. Klicken Sie in der Menüleiste auf **Global Access**.
3. Geben Sie gegebenenfalls Ihre E-Mail-Adresse und Ihr Kennwort für Seagate Global Access ein.
4. Klicken Sie auf **Melden Sie sich bei Ihrem Konto an**.

Einzelheiten dazu, wie Sie anderen Personen Zugriff auf Ihre private Freigabe geben können, finden Sie in der Dokumentation zu Global Access.

Anschließen eines USB-Druckers an den BlackArmor-Server

Hinweis: Dies ist ein optionaler Schritt. Drucker können nur von BlackArmor-Administratoren eingerichtet werden.

Sie können einen USB-Drucker im lokalen Netzwerk verfügbar machen, indem Sie ihn an den Server anschließen.

So schließen Sie einen Drucker an:

1. Vergewissern Sie sich, dass der Drucker ausgeschaltet ist.
2. Schließen Sie den Drucker mit einem hochwertigen USB-Kabel an einen der USB-Anschlüsse an der Rückseite des BlackArmor-Servers an.
3. Schalten Sie den Drucker ein und installieren Sie gegebenenfalls den Treiber gemäß den Herstelleranweisungen auf Ihrem Computer.
4. Weisen Sie die anderen Benutzer im lokalen Netzwerk an, den USB-Drucker gemäß den Anweisungen für ihr Betriebssystem zur Liste ihrer verfügbaren Drucker hinzuzufügen.

Der Drucker steht jetzt allen BlackArmor-Benutzern zur Verfügung. Den Drucker-Manager finden Sie in BlackArmor Manager im Menü „Netzwerk“. Weitere Informationen finden Sie in der Onlinehilfe.

Einrichten des BlackArmor-Servers als Media Server

Hinweis: Dies ist ein optionaler Schritt. Die Media-Server-Funktion kann nur von BlackArmor-Administratoren eingerichtet werden.

Sie können den BlackArmor-Server nutzen, um digitale Fotos, Videos und Musik für Benutzer im lokalen Netzwerk verfügbar zu machen. Die Ordner, in denen Ihre Mediendateien abgelegt werden („Gemeinsame Bilder“, „Gemeinsame Musik“ und „Gemeinsame Videos“) sind verfügbar, wenn Sie in BlackArmor Manager die Drag&Sort-Funktion aktiviert haben. Weitere Informationen finden Sie in der Onlinehilfe von BlackArmor Manager.

So richten Sie den BlackArmor-Server als Media Server ein:

1. Klicken Sie in der Menüleiste auf **Medien** und dann auf **Mediendienst**.
2. Wählen Sie neben **Dienst** die Option **Aktivieren**.
3. Legen Sie gegebenenfalls die Sortiermethode für Mediendateien fest und klicken Sie dann auf **Senden**.

Sie können den BlackArmor-Server als iTunes-Server einrichten, um den BlackArmor-Benutzern das Streaming von Musik zu einem Netzwerkcomputer mit iTunes-Software oder einem iPod®, der an einen Netzwerkcomputer angeschlossen ist, zu ermöglichen.

4. Legen Sie fest, wie oft der Server nach neuer Musik suchen soll. Sie können einen Zeitabstand zwischen fünf Minuten und einem Tag wählen.
5. Klicken Sie auf **Senden**, um die Einstellungen zu speichern.

Der Mediendienst wird aktiviert.

Erstellen von Multimedia-Ordnern

Führen Sie folgende Schritte aus, um die Media Server-Ordner zu erstellen:

1. Starten Sie BlackArmor Discovery.
2. Wählen Sie den Server aus:

- (Windows) Wählen Sie den Server aus und klicken Sie auf **Laufwerkinfos anzeigen**.
- (Mac) Wählen Sie in der oberen Tabelle des Discovery-Fensters den Server aus und in der unteren Tabelle die öffentliche Freigabe, und klicken Sie dann auf **Freigabe verbinden**.

3. Wählen Sie die öffentliche Freigabe aus und klicken Sie auf **Ansicht** (Windows) oder doppelklicken Sie auf die verbundene Freigabe (Mac).

Die Freigabe wird geöffnet.

4. Erstellen Sie die folgenden Ordner: „Gemeinsame Musik“, „Gemeinsame Bilder“, „Gemeinsame Videos“.

Jetzt können Sie Dateien, die anderen zur Verfügung stehen sollen, in den entsprechenden Ordnern bereitstellen.

Nächste Schritte für Administratoren

Bevor Sie fortfahren, sollten Sie sich anhand dieses Handbuchs mit den Funktionen von BlackArmor-Server und -Software vertraut machen.

Die Standardeinstellungen des BlackArmor-Servers sind auf typische Nutzungsanforderungen ausgelegt, sodass Sie sofort mit dem Speichern, Freigeben und Sichern von Dateien beginnen können (siehe Seite 29). Mit BlackArmor Manager können Sie die Einstellungen des BlackArmor-Servers nach Bedarf anpassen.

Nach der Ersteinrichtung können Sie folgende Aufgaben ausführen:

- Erstellen von Gruppenkonten, um die Verwaltung von Zugriffsberechtigungen zu erleichtern (siehe Seite 36).
- Einrichten der Datenträger und RAID-Konfigurationen (siehe Seite 31).
- Einrichten der laufenden Archivsicherung auf einen zweiten Server im Netzwerk (siehe Seite 37).
- Speichern aller Foto-, Video- und Musikdateien auf dem Server und Einrichten des Servers als Media Server, damit Multimedia-Player im Netzwerk auf die Dateien zugreifen können (siehe Seite 39).
- Überwachen des Servers vor Ort oder aus der Ferne (siehe Seite 39).

In den übrigen Kapiteln dieses Handbuchs finden Sie Informationen über die Funktionen des Servers und Empfehlungen dazu, wie Sie ein Speichersystem einrichten können, das Ihren Bedürfnissen entspricht.

Hinweis: Vergessen Sie nicht, dass Sie auch ein BlackArmor-Benutzer sind. Fahren Sie mit Erste Schritte für BlackArmor-Benutzer fort, um Ihre eigenen Dateien zu speichern, zu sichern und für andere verfügbar zumachen.

Erste Schritte für BlackArmor-Benutzer

Führen Sie die Schritte in diesem Abschnitt aus, um den BlackArmor-Server für die Nutzung einzurichten.

1. Vergewissern Sie sich, dass Sie Folgendes vom BlackArmor-Administrator erhalten haben:
   - BlackArmor Discovery-Software
   - BlackArmor-Benutzername und -Kennwort
   - BlackArmor Backup-Software (optional)
   - Namen der Freigaben, auf die Sie zugreifen können
   - Angaben zu etwaigen Zugriffseinschränkungen (z. B. nur Lesezugriff auf eine bestimmte Freigabe)
   - BlackArmor NAS 440/420-Benutzerhandbuch
2. Installieren Sie die BlackArmor-Software.

   Installieren Sie BlackArmor Discovery *und* BlackArmor Backup, falls Sie nicht bereits eine andere Sicherungssoftware verwenden.
3. Stellen Sie mit BlackArmor Discovery eine Verbindung zum BlackArmor-Server und den Freigaben her, auf die Sie Zugriff haben.
   - (Windows) Doppelklicken Sie auf das BlackArmor Discovery-Symbol auf dem Desktop.
   - (Mac) Doppelklicken Sie auf das BlackArmor Discovery-Symbol im Ordner „Anwendungen“.

   Beim Start sucht BlackArmor Discovery automatisch nach BlackArmor-Servern im lokalen Netzwerk und zeigt diese in einer Liste an.
4. Wählen Sie den neuen BlackArmor-Server aus.

   Eine Liste der Freigaben auf dem Server wird angezeigt (Mac). Klicken Sie auf **Server verwalten**.
   - (Windows) Klicken Sie auf **Laufwerkinfos anzeigen**. Eine Liste der Freigaben auf dem Server wird angezeigt.

5. Verwenden Sie die Pfeile nach oben und unten, um in der Liste der Freigaben zu blättern, und führen Sie nach Bedarf folgende Schritte aus:
   - Klicken Sie auf **Verwalten** und geben Sie Ihren Benutzernamen und Ihr Kennwort ein, um mit BlackArmor Manager auf den Server zuzugreifen. Falls Sie Ihren Benutzernamen und Ihr Kennwort nicht kennen, wenden Sie sich an Ihren Administrator.
   - Wählen Sie eine Freigabe aus und klicken Sie auf **Ansicht**, um die Freigabe anzuzeigen.
   - Wählen Sie eine Freigabe aus und klicken Sie auf **Verbinden**, um die Freigabe zu verbinden.
     - Wenn Sie dazu aufgefordert werden, geben Sie Ihren BlackArmor-Benutzernamen und Ihr Kennwort ein. Die Verbindung zum freigegebenen Ordner wird hergestellt und sein Symbol erscheint auf dem Schreibtisch (Mac).
     - (Windows) Wählen Sie im Dropdownmenü einen Laufwerksbuchstaben aus und klicken Sie auf **Ja**. Der Freigabe wird der gewählte Laufwerksbuchstabe zugewiesen. Die Freigabe wird in Windows Explorer unter diesem Laufwerksbuchstaben angezeigt.
   - Falls Sie Zugriff auf mehrere Freigaben haben, verbinden Sie diese nach Bedarf auf dieselbe Weise.

   Hinweis: Sie können beliebig viele öffentliche und private Freigaben verbinden. Wenn mehrere *private* Freigaben verbunden werden sollen, müssen diese jedoch dieselben Authentifizierungsdaten besitzen.

6. Speichern Sie Ihre Dateien in Freigaben, auf die andere Benutzer über das lokale Netzwerk oder das Internet zugreifen können.

Optionale Schritte

- *(Optional)* Erstellen Sie eine vollständige Sicherung Ihrer wichtigen Dateien oder richten Sie regelmäßige Sicherungen ein. Verwenden Sie dazu BlackArmor Backup (siehe Seite 50).
- *(Optional)* Falls ein USB-Drucker an den BlackArmor-Server angeschlossen ist, fügen Sie diesen gemäß den Anweisungen für Ihr Betriebssystem zur Liste der verfügbaren Drucker hinzu.
- *(Optional)* Falls der BlackArmor-Administrator den Mediendienst auf dem Server eingerichtet hat und Sie Zugriff auf die Freigabe mit den Musikdateien haben, installieren Sie iTunes auf Ihrem Computer und folgen Sie den iTunes-Anweisungen zum Streaming von Musik.
- *(Optional)* Falls der BlackArmor-Administrator Global Access auf dem Server aktiviert hat, richten Sie ein kostenloses Global Access-Konto ein, damit Sie über das Internet auf die Dateien auf dem BlackArmor-Server zugreifen können. Siehe „Erstellen eines Seagate Global Access-Kontos“ auf Seite 26.

Erstellen eines Seagate Global Access-Kontos

Seagate Global Access ist ein Service, über den Sie die Dateien auf dem BlackArmor-Server von jedem Ort aus anzeigen, herunterladen, freigeben und bearbeiten können, Dateien in einer privaten Freigabe verfügbar machen können und Dateien für Personen außerhalb Ihres Netzwerks freigeben können.

So richten Sie ein Seagate Global Access-Konto ein:

1. Öffnen Sie die Seagate Global Access-Website unter *http://globalaccess.seagate.com*.
2. Die Anmeldeseite von Seagate Global Access wird angezeigt. Klicken Sie auf den Link, um zu beginnen.
3. Geben Sie auf der Anmeldeseite von Seagate Global Access unter **Sie haben noch kein Konto?** Ihre E-Mail-Adresse ein und klicken Sie auf **Senden**.
4. Die Seite wird aktualisiert und Sie werden informiert, dass eine E-Mail an Sie versandt wurde.

Global Access schickt eine Einladung an die angegebene E-Mail-Adresse; diese enthält einen Link zu einer Webseite, auf der Sie ein Global Access-Konto einrichten können. Folgen Sie den Online-Anweisungen, um das Konto einzurichten und sich bei Global Access anzumelden.

Klicken Sie auf der Global Access-Website auf **Hilfe**, um Informationen zur Verwendung von Seagate Global Access zu erhalten.

4. Optimale Nutzung des BlackArmor®-Servers

- Einführung
- Die Rolle des BlackArmor-Administrators
- Standardeinstellungen des BlackArmor-Servers
- Verwalten von Datenträgern, Freigaben und Speicher des BlackArmor-Servers
- Verwalten von BlackArmor-Benutzern
- Netzwerksicherung der Dateien auf dem BlackArmor-Server
- Einrichten der Link Aggregation
- Einrichten des BlackArmor-Servers als Media Server
- Überwachen des BlackArmor-Servers
- Ändern der erweiterten Einstellungen des BlackArmor-Servers
- Warten des BlackArmor-Servers

Einführung

Dieses Kapitel beschreibt die Funktionen von BlackArmor®-Server und -Software und gibt BlackArmor-Administratoren Tipps zu ihrer Nutzung.

Einige Funktionen des BlackArmor-Servers sollten möglichst nur von Administratoren verwendet werden, die erfahrene Computerbenutzer sind. Abschnitte zu solchen Funktionen sind deutlich gekennzeichnet.

Hinweis: Die in diesem Kapitel beschriebenen Aufgaben können nur von BlackArmor-Administratoren ausgeführt werden. Falls Sie kein BlackArmor-Administrator sind, gehen Sie zu Kapitel 5 „Tipps für BlackArmor®-Benutzer“ auf Seite 47.

Die Rolle des BlackArmor-Administrators

BlackArmor-Administratoren haben vollen Zugriff auf alle Funktionen und Einstellungen des BlackArmor-Servers und alle darauf gespeicherten Dateien.

Die Rolle des BlackArmor-Administrators beinhaltet folgende Aufgaben:

- Verwaltung des Speicherplatzes auf dem BlackArmor-Server durch die die Erstellung und Bearbeitung von Datenträgern und Freigaben (siehe Seite 30).
- Steuerung des Zugriffs auf den Server durch die Erstellung und Verwaltung von BlackArmor-Benutzerkonten (siehe Seite 36).
- Gewährleistung des reibungslosen Betriebs des BlackArmor-Servers durch die Überwachung des Zustands von Server und Festplatten (siehe Seite 39).
- Gewährleistung des reibungslosen Betriebs des BlackArmor-Servers durch die Aktualisierung der Firmware, wenn neue Versionen verfügbar sind (siehe Seite 46).

Als BlackArmor-Administrator können Sie außerdem die Nutzung des BlackArmor-Servers wie folgt optimieren:

- Erstellen von Gruppenkonten, um die Steuerung des Zugriffs auf Freigaben zu erleichtern. Mit Benutzergruppen können Sie den Zugriff auf Freigaben für einzelne Benutzer oder ganze Gruppen in einem Fenster bearbeiten (siehe Seite 36).
- Einrichtung der laufenden Archivsicherung aller Daten auf dem BlackArmor-Server, um die Dateien auf dem Server zu schützen (siehe Seite 37).
- Einrichtung der *Link Aggregation*, bei der beide LAN-Anschlüsse mit dem Netzwerk verbunden werden, um die Ausfallsicherheit zu erhöhen (siehe Seite 39).
- Einrichtung des BlackArmor-Servers als Media Server, um den BlackArmor-Benutzern das Streaming von Musik zu Netzwerkcomputern mit iTunes zu ermöglichen (siehe Seite 39).
- Einrichtung der Energiesparfunktion, sodass die Festplatten im BlackArmor-Server bei Inaktivität *heruntergefahren* (angehalten) und in den Standby-Modus versetzt werden, um Energie – und Stromkosten – zu sparen (siehe Seite 43).
- Anschließen einer unterbrechungsfreien Stromversorgung, die bei einem Stromausfall die Versorgung lange genug gewährleistet, um geöffnete Dateien zu speichern und den BlackArmor-Server ordnungsgemäß herunterzufahren (siehe Seite 43).
- *(Erfahrene Benutzer)* Einrichtung von Dynamic DNS in BlackArmor Manager, um sicherzustellen, dass der eingehende Netzwerkverkehr an sein Ziel gelangt (siehe Seite 42).

Die übrigen Abschnitte dieses Kapitels beschreiben die Standardeinstellungen des BlackArmor-Servers und erklären, wie Sie die Einstellungen ändern und andere Funktionen des Servers nutzen können, um die optimale Speicherlösung für Ihre Anforderungen einzurichten.

Standardeinstellungen des BlackArmor-Servers

Die Standardeinstellungen des BlackArmor-Servers sind auf typische Nutzungsanforderungen ausgelegt, sodass Sie unmittelbar beginnen können, Ihre Dateien zu speichern, zu sichern und für andere verfügbar zu machen:

- **Benutzerkonten**: Der BlackArmor-Server verfügt über ein vorkonfiguriertes Benutzerkonto für den Administrator, für das Sie bei der Ersteinrichtung ein eigenes Kennwort angeben können (siehe Seite 17). Mit BlackArmor Manager können Sie außerdem nach Bedarf neue Benutzerkonten anlegen (siehe Seite 36).
- **Freigaben**: Auf dem BlackArmor-Server sind zwei Freigaben vorkonfiguriert: Download und Öffentlich. Sie können die Einstellungen dieser Freigaben an Ihre Bedürfnisse anpassen oder mit BlackArmor Manager neue öffentliche und private Freigaben einrichten (siehe Seite 33).
- **RAID-Konfiguration**: Standardmäßig verwendet der BlackArmor-Server eine RAID-5-Konfiguration, wenn vier Festplatten installiert sind. RAID 5 steht für Redundant Array of Independent Disks (redundante Anordnung unabhängiger Festplatten) der Stufe 5. Diese Technologie schützt durch Redundanz die Daten in Ihrem Speichersystem gegen Festplattenausfälle und andere Katastrophen.

Falls gewünscht können Sie auch eine andere RAID-Konfiguration verwenden. Neben RAID 5 bieten auch RAID 1 und RAID 10 Datensicherheit. RAID 5 ist jedoch die empfohlene Konfiguration, da sie den besten Schutz für den BlackArmor-Server bietet. Die RAID-Konfiguration des Servers sollte nur von Benutzern geändert werden, die mit der RAID-Technik vertraut sind.

Weitere Informationen finden Sie auf Seite 31.

- **Netzwerkeinstellungen**: Der BlackArmor-Server unterstützt zwar die gleichzeitige Nutzung von zwei Netzwerkverbindungen zur schnelleren Datenübertragung; sie müssen aber *nicht* beide LAN-Anschlüsse mit dem Netzwerk verbinden, um mit dem Server arbeiten zu können. Weitere Informationen finden Sie auf Seite 39.

Standardmäßig verwendet der Server außerdem den Netzwerkmodus DHCP. Dies ist der empfohlene Modus. *DHCP* steht für Dynamic Host Configuration Protocol (dynamisches Protokoll für die Host-Konfiguration), ein Verfahren, bei dem allen Systemen in einem Netzwerk automatisch IP-Adressen zugewiesen werden. (Beim statischen Modus müssen alle IP-Adressen manuell zugewiesen und geändert werden.)

Falls Sie nicht in einem Großunternehmen mit eigener IT-Abteilung arbeiten, empfiehlt Seagate, den DHCP-Netzwerkmodus zu verwenden.

- **Administratorkennwort**: Die Standard-Anmeldeinformationen für den Server lauten:

  Benutzername: admin

  Kennwort: admin

Bei der Ersteinrichtung des Servers haben Sie die Möglichkeit, das Administratorkennwort zu ändern. Falls Sie dies nicht getan haben oder das Kennwort erneut ändern möchten, rufen Sie BlackArmor Manager auf (siehe Seite 16). Wählen Sie im Menü „System“ die Option **Admin-Kennwort**, um das Administratorkennwort zu ändern. Eine schrittweise Anleitung zur Änderung des Kennworts finden Sie in der Onlinehilfe von BlackArmor Manager.

Falls der Server auf die Werkseinstellungen zurückgesetzt wird, müssen Sie wieder die Standardanmeldeinformationen verwenden.

- **Global Access**: Der BlackArmor-Server ist standardmäßig nicht für den Zugriff über das Internet eingerichtet. Aktivieren Sie Seagate Global Access, wenn Sie von jedem Ort aus auf die Dateien auf dem BlackArmor-Server zugreifen oder Ihre Dateien für Personen außerhalb des Netzwerks, wie etwa Kunden oder Freunde, verfügbar machen möchten (siehe Seite 20).
- **Download-Tool**: Die Standardeinstellungen des BlackArmor-Servers gestatten das Herunterladen großer Dateien aus dem Internet mit dem Download-Tool von BlackArmor Manager zu jeder Zeit. Mit BlackArmor Manager können Sie die Größe und Zahl gleichzeitiger Downloads begrenzen und Downloads aus dem Internet auf bestimmte Tage und Zeiten beschränken (siehe Seite 35).
- **Media Server**: Standardmäßig ist der BlackArmor-Server nicht als Media Server eingerichtet. Mit BlackArmor Manager können Sie den Server als Media Server einrichten, um Digitalfotos, Videos und Musik im lokalen Netzwerk verfügbar zu machen, und den iTunes-Dienst aktivieren, um BlackArmor-Benutzern das Streaming von Musik zu Netzwerkcomputern mit iTunes zu ermöglichen (siehe Seite 22).

Verwalten von Datenträgern, Freigaben und Speicher des BlackArmor-Servers

Dieser Abschnitt behandelt folgende Themen:

- Übersicht über Datenträger und Freigaben
- Verwalten von Datenträgern
- Verwalten von Freigaben
- Festlegen von Speicherplatzbegrenzungen für BlackArmor-Benutzer
- Festlegen von Kulanzzeiten für Kontingente
- Steuerung von Downloads aus dem Internet auf den BlackArmor-Server

Übersicht über Datenträger und Freigaben

Standardmäßig ist auf dem BlackArmor-Server ein Datenträger mit zwei Freigaben eingerichtet: Download und Öffentlich. Ein *Datenträger* ist ein Speicherbereich, der einen Teil einer Festplatte, eine ganze Festplatte oder mehrere Festplatten umfassen kann. Eine *Freigabe* ist ein Ordner. Freigaben werden innerhalb von Datenträgern erstellt.

Standarddatenträger und -freigaben sind auf typische Nutzungsanforderungen ausgelegt, sodass Sie unmittelbar beginnen können, Ihre Dateien zu speichern, zu sichern und für andere verfügbar zu machen. Als BlackArmor-Administrator können Sie aber auch mit BlackArmor Manager weitere Datenträger und Freigaben auf dem BlackArmor-Server erstellen, falls Sie den verfügbaren Speicher in kleinere Bereiche unterteilen möchten, die sie unterschiedlichen Benutzern zuweisen können.

Sie könnten beispielsweise drei Datenträger erstellen, auf denen verschiedene Arten von Daten gespeichert werden:

- Datenträger A: Geschäftsdateien
- Datenträger B: Sicherungsdateien
- Datenträger C: Mediendateien

Anschließend könnten Sie entsprechend Ihren Bedürfnissen auf jedem Datenträger einen oder mehrere Ordner (Freigaben) erstellen:

- Datenträger A: Geschäftsdateien
  - Freigabe 1: Kundendateien
  - Freigabe 2: Finanzdateien
  - Freigabe 3: Personaldateien
- Datenträger B: Sicherungsdateien
  - Freigabe 1: Tägliche Sicherungen
  - Freigabe 2: Monatliche Sicherungen
- Datenträger C: Mediendateien
  - Freigabe 1: Musikdateien
  - Freigabe 2: Fotodateien
  - Freigabe 3: Videodateien

Verwalten von Datenträgern

Standardmäßig ist für den verfügbaren Speicher im BlackArmor-Server ein Datenträger mit RAID-5-Konfiguration eingerichtet.

Übersicht über RAID

RAID steht für Redundant Array of Independent Disks (redundante Anordnung unabhängiger Festplatten). Diese Technologie schützt durch Redundanz die Daten in Ihrem Speichersystem gegen Festplattenausfälle und andere Katastrophen.

Es gibt verschiedene RAID-Konfigurationen, die sich darin unterscheiden, wie viel Schutz sie bieten (und auf welche Weise) und wie viele Festplatten verwendet werden können.

Standardmäßig verwendet der BlackArmor-Server eine RAID-5-Konfiguration, die Ihre Daten nicht nur sicher speichert, sondern zudem redundante Informationen – sogenannte *Paritätsinformationen* – verwendet, anhand derer Ihre Dateien bei Ausfall einer Festplatte im Server rekonstruiert werden können.

Sie können eine andere RAID-Konfiguration für Ihre Datenträger verwenden – der BlackArmor-Server unterstützt RAID 0, 1, 5 und 10 sowie JBOD (Just a Bunch of Disks – nur ein Haufen Festplatten). RAID 5 ist jedoch die empfohlene Konfiguration, da sie den besten Schutz für den BlackArmor-Server bietet.

Die folgende Tabelle beschreibt die verschiedenen RAID-Konfigurationen, die der BlackArmor-Server unterstützt.

Tabelle 1: Unterstützte RAID-Konfigurationen für Datenträger

RAID-Konfiguration des Datenträgers	Anzahl der erforderlichen Festplatten	Beschreibung
RAID 0 (auch als „Striping“ bezeichnet)	2 – 4	Ein Datenträger, bei dem die Daten in gleich großen Blöcken („Streifen“) über die Festplatten verteilt werden. Ein Stripesetdatenträger bietet keine Datenredundanz und damit *keine Datensicherheit*.
RAID 1 (auch als „Spiegelung“ bezeichnet)	2	Ein Datenträger, bei dem auf zwei Festplatten die gleichen Daten gespeichert (gespiegelt) werden. Bietet Datensicherheit.
RAID 5	3 – 4	Bei der RAID-5-Konfiguration sorgen Striping und Paritätsinformationen für Redundanz. (Paritätsinformationen dienen zur Rekonstruktion der Daten bei Ausfall einer Festplatte. Bei RAID 5 werden die Paritätsinformationen gleichmäßig auf die Festplatten mit den gespeicherten Daten verteilt.)
RAID 10	4	Ein Datenträger mit RAID-10-Konfiguration besteht aus mehreren gleich großen RAID-0-Datenträgern. Bei RAID 10 werden sowohl Striping als auch Spiegelung verwendet.
Span (auch als „JBOD“[a] bezeichnet)	1 – 4	Eine Gruppe von Festplatten in einem Server *ohne Schutz durch RAID*.

a.„Just a Bunch of Disks“ (nur ein Haufen Festplatten)

Die RAID-Konfiguration des Servers sollte nur von Benutzern geändert werden, die mit der RAID-Technik vertraut sind.

Erstellen neuer Datenträger

Als BlackArmor-Administrator können Sie mit BlackArmor Manager nach Bedarf Freigaben auf dem Standarddatenträger einrichten oder weitere Datenträger erstellen. Bei der Erstellung eines Datenträgers können Sie folgende Punkte festlegen:

- Größe des Datenträgers
- zu verwendende Festplatten
- RAID-Konfiguration (siehe Seite 31)

Sie können dieselben Festplatten für mehrere Datenträger verwenden, solange auf den Festplatten ausreichend Platz verfügbar ist. So könnten Sie beispielsweise eine Hälfte des Speicherplatzes auf den Festplatten 1, 2 und 3 für Datenträger A verwenden und die andere Hälfte für Datenträger B.

Zur Erstellung eines neuen Datenträgers rufen Sie BlackArmor Manager auf (siehe Seite 16). Datenträger finden Sie im Menü „Speicher“. Weitere Informationen zu Datenträgern sowie zum Löschen und Bearbeiten von Datenträgern finden Sie in der Onlinehilfe.

Verwalten von Freigaben

Freigaben auf dem BlackArmor-Server können öffentlich (mit gewissen Einschränkungen für jeden zugänglich) oder privat (auf bestimmte Benutzerkonten beschränkt) sein.

Als BlackArmor-Administrator können Sie Freigaben jederzeit nach Bedarf erstellen, ändern oder löschen. Beachten Sie aber, dass beim Löschen einer Freigabe auch alle darin enthaltenen Dateien gelöscht werden. Daher sollten Sie vorsichtig sein, wenn Sie Freigaben vom BlackArmor-Server löschen.

Private Freigaben

Eine private Freigabe ist einem Benutzerkonto zugeordnet und der Zugriff auf eine solche Freigabe ist nur BlackArmor-Benutzern mit der entsprechenden Berechtigung gestattet. Private Freigaben sind durch ein Kennwort geschützt. (Als BlackArmor-Administrator können Sie eine private Freigabe mit BlackArmor Manager in eine öffentliche Freigabe verwandeln.)

Der Zugriff auf eine Freigabe kann folgendermaßen eingeschränkt werden:

- Sie können den Zugriff auf bestimmte BlackArmor-Benutzer beschränken.
- Sie können bestimmte BlackArmor-Benutzer auf reinen Lesezugriff beschränken. Bei *Lesezugriff* kann der BlackArmor-Benutzer die Dateien in der Freigabe anzeigen, aber keine Dateien bearbeiten oder in der Freigabe speichern.
- Sie können BlackArmor-Benutzern Vollzugriff auf die Freigabe gewähren. Damit können sie ihre Dateien in der Freigabe speichern und sichern sowie Dateien in der Freigabe bearbeiten und auf ihren Computer oder ein an den Server angeschlossenes USB-Laufwerk herunterladen (siehe Seite 51).

Der Besitzer einer Freigabe kann außerdem mit Global Access anderen Personen Zugriff auf einzelne oder alle Dateien in der privaten Freigabe geben. Siehe Seite 25.

Hinweis: Wenn mehrere *private* Freigaben gleichzeitig verbunden werden sollen, müssen diese dieselben Authentifizierungsdaten besitzen.

Private Freigaben werden als Teil eines BlackArmor-Benutzerkontos erstellt. Zur Erstellung einer privaten Freigabe rufen Sie BlackArmor Manager auf (siehe Seite 16). Benutzerkonten finden Sie im Menü „Zugriff“.

Zur Änderung der Berechtigungseinstellungen einer Freigabe rufen Sie BlackArmor Manager auf (siehe Seite 16). Freigabeberechtigungen finden Sie im Menü „Zugriff“.

Schrittweise Anleitungen zur Verwendung von BlackArmor Manager finden Sie in der Onlinehilfe.

Öffentliche Freigaben

Öffentliche Freigaben unterliegen keinen Einschränkungen. BlackArmor-Benutzer können beliebig viele öffentliche Freigaben verbinden.

Zur Erstellung einer öffentlichen Freigabe rufen Sie BlackArmor Manager auf (siehe Seite 16). Freigaben finden Sie im Menü „Speicher“. Schrittweise Anleitungen zur Verwendung von BlackArmor Manager finden Sie in der Onlinehilfe.

Besondere Funktionen für Freigaben

Diese Funktionen sind für alle Freigaben verfügbar. Sie können je nach Einsatzzweck der Freigabe aktiviert oder deaktiviert werden.

- **Unterstützung für Dateiprotokolle**: Zur gemeinsamen Nutzung von Dateien auf verschiedenen Computern in einem Netzwerk werden standardisierte Dateiprotokolle verwendet. Sie können die Unterstützung einiger oder aller der folgenden Protokolle aktivieren:
  - **CIFS**: Common Internet File System (allgemeines Internet-Dateisystem). Ermöglicht die gemeinsame Nutzung von Dateien durch Benutzer mit unterschiedlichen Windows-Computern, ohne dass spezielle Software installiert werden muss.
  - **FTP**: File Transfer Protocol (Dateiübertragungsprotokoll). Ermöglicht den sicheren Austausch von Dateien zwischen dem BlackArmor-Server und anderen Computern über das Internet.
  - **NFS**: Network File System (Netzwerkdateisystem). Ermöglicht die gemeinsame Nutzung von Dateien mit Linux- oder UNIX-Computern oder Computern mit NFS-Client-Software.
- **Papierkorb-Dienst**: Sie können die Dateien in einer Freigabe schützen, indem Sie den BlackArmor Manager-Papierkorb aktivieren. Wenn der Papierkorb für eine Freigabe aktiviert ist, bewahrt BlackArmor Manager Dateien auf, die von der Freigabe gelöscht werden, sodass sie bei Bedarf wiederhergestellt werden können.
- **Drag&Sort-Dienst**: Sie können für eine Freigabe einrichten, dass Mediendateien je nach Dateityp automatisch in bestimmte Ordner auf den Computern der BlackArmor-Benutzer heruntergeladen werden. Zum Beispiel könnten heruntergeladene Musikdateien automatisch im Ordner „Musik“ abgelegt werden.

Zur Aktivierung oder Deaktivierung dieser Funktionen rufen Sie BlackArmor Manager auf (siehe Seite 16). Freigaben finden Sie im Menü „Speicher“. Schrittweise Anleitungen zur Verwendung von BlackArmor Manager finden Sie in der Onlinehilfe.

Festlegen von Speicherplatzbegrenzungen für BlackArmor-Benutzer

Standardmäßig gelten keine Begrenzungen für den Speicherplatz, den Benutzer auf dem BlackArmor-Server belegen können (abgesehen von der Größe des für den Benutzer eingerichteten Datenträgers).

Als BlackArmor-Administrator können Sie jedoch Speicherplatzbegrenzungen für Benutzerkonten und Freigaben festlegen. Sie können unterschiedliche Begrenzungen für einzelne Benutzerkonten oder für einzelne Freigaben, auf die ein Benutzer Zugriff hat, festlegen. Sie können auch Begrenzungen für manche Benutzerkonten, aber nicht für andere festlegen.

Wenn ein BlackArmor-Benutzer die Grenzen des ihm zugeteilten Speicherplatzes erreicht hat, müssen ältere oder nicht mehr benötigte Dateien durch einen BlackArmor-Administrator gelöscht werden, um Platz für weitere Dateien zu schaffen.

Zum Festlegen von Speicherplatzbegrenzungen für BlackArmor-Benutzer rufen Sie BlackArmor Manager auf (siehe Seite 16). Speicherplatzbegrenzungen werden auf der Seite „Kontingent“ im Menü „Speicher“ festgelegt. Schrittweise Anleitungen zur Verwendung von BlackArmor Manager finden Sie in der Onlinehilfe.

Festlegen von Kulanzzeiten für Kontingente

Als BlackArmor-Administrator können Sie eine Kulanzzeit festlegen, in der die Speicherplatzbegrenzung eines Kontingents vorübergehend überschritten werden darf, Wenn das Kontingent erreicht ist, können Sie vorübergehend weitere 100 Megabyte (MB) Speicherplatz gewähren, damit Benutzer Zeit haben zu entscheiden, welche Dateien Sie behalten möchten.

Nach der Kulanzzeit können keine weiteren Dateien mehr gespeichert werden, bis wieder Platz verfügbar gemacht wird.

Zum Festlegen der Kulanzzeit für gespeicherte Dateien rufen Sie BlackArmor Manager auf (siehe Seite 16). Die Kulanzzeit wird auf der Seite „Kontingent“ im Menü „Speicher“ festgelegt. Weitere Informationen finden Sie in der Onlinehilfe von BlackArmor Manager.

Steuerung von Downloads aus dem Internet auf den BlackArmor-Server

BlackArmor Manager beinhaltet ein spezielles Tool für das Herunterladen großer Dateien von FTP- und anderen Sites im Internet direkt auf den Server. Das Download-Tool gibt BlackArmor-Administratoren die Möglichkeit zu steuern, wann große Downloads ausgeführt werden, sodass der Server nicht überlastet wird.

Das Download-Tool stellt Download-Aufträge in eine Warteschlange und die Aufträge werden in der Reihenfolge ausgeführt, in der sie in der Warteschlange stehen. Falls ein Auftrag nicht ganz oben steht, wird er nicht sofort ausgeführt. Als BlackArmor-Administrator können Sie Aufträge in der Warteschlange nach oben oder unten verschieben.

Außerdem können Sie einschränken, wann Download-Aufträge ausgeführt werden und wie viele gleichzeitig stattfinden können (nie mehr als drei). Sie können festlegen, dass Downloads nur abends, am Wochenende oder zu anderen ruhigen Zeiten in der Woche ausgeführt werden sollen.

Überlegen Sie, wie viel Bandbreite der BlackArmor-Server zur Verfügung hat und welchen Anteil dieser Bandbreite Sie für lange Downloads aufgeben möchten. Nehmen Sie die entsprechenden Einschränkungen vor, um zu verhindern, dass mehrere große Dateien gleichzeitig oder zu Zeiten, in denen der BlackArmor-Server mit anderen Aufgaben beschäftigt ist, heruntergeladen werden.

Um die Download-Tool-Einstellungen des BlackArmor-Servers zu ändern oder die Warteschlange anzuzeigen und die Rangfolge der vorhandenen Aufträge zu ändern, rufen Sie BlackArmor Manager auf (siehe Seite 16). Die Download-Verwaltung finden Sie im Menü „Speicher“. Schrittweise Anleitungen zur Verwendung von BlackArmor Manager finden Sie in der Onlinehilfe.

Verwalten von BlackArmor-Benutzern

Dieser Abschnitt behandelt die Merkmale von Benutzerkonten und gibt einen Überblick über die Einrichtung neuer Benutzerkonten mit BlackArmor Manager. Schrittweise Anleitungen zur Verwendung von BlackArmor Manager finden Sie in der Onlinehilfe.

Verwalten von Benutzerkonten

Jeder Benutzer, der den BlackArmor-Server nutzen soll, benötigt ein eigenes Benutzerkonto. Für den Zugriff auf einen öffentlich verfügbar gemachten Ordner ist aber kein Benutzerkonto erforderlich. Als BlackArmor-Administrator können Sie die einzelnen Benutzerkonten an die Bedürfnisse des jeweiligen BlackArmor-Benutzers anpassen. (Weitere Informationen finden Sie unter „Erstellen von Benutzerkonten“ auf Seite 19.)

Dabei haben Sie folgende Möglichkeiten:

- Sie können dem BlackArmor-Benutzer Administratorberechtigungen geben.
- Sie können den Benutzer zu einer Benutzergruppe hinzufügen (siehe nächster Abschnitt).
- Sie können eine private Freigabe für den Benutzer erstellen.

Nachdem ein Benutzerkonto erstellt wurde, kann es jederzeit wieder geändert oder gelöscht werden.

Zum Erstellen, Ändern oder Löschen eines Benutzerkontos rufen Sie BlackArmor Manager auf (siehe Seite 16). Benutzerkonten finden Sie im Menü „Zugriff“. Schrittweise Anleitungen zur Verwendung von BlackArmor Manager finden Sie in der Onlinehilfe.

Erstellen und Bearbeiten von Benutzergruppen

Durch die Einteilung von BlackArmor-Benutzern in Gruppen lässt sich der Zugriff auf Freigaben schneller und einfacher verwalten. Dabei können Sie die Zugriffsberechtigungen für einzelne Benutzer oder ganze Gruppen in einem einheitlichen Fenster bearbeiten.

Zur Erstellung von Benutzergruppen richten Sie in BlackArmor Manager das Gruppenkonto ein und fügen anschließend Benutzer zur Gruppe hinzu. Teilen Sie die BlackArmor-Benutzer danach in Gruppen ein, auf welche Freigaben sie zugreifen müssen.

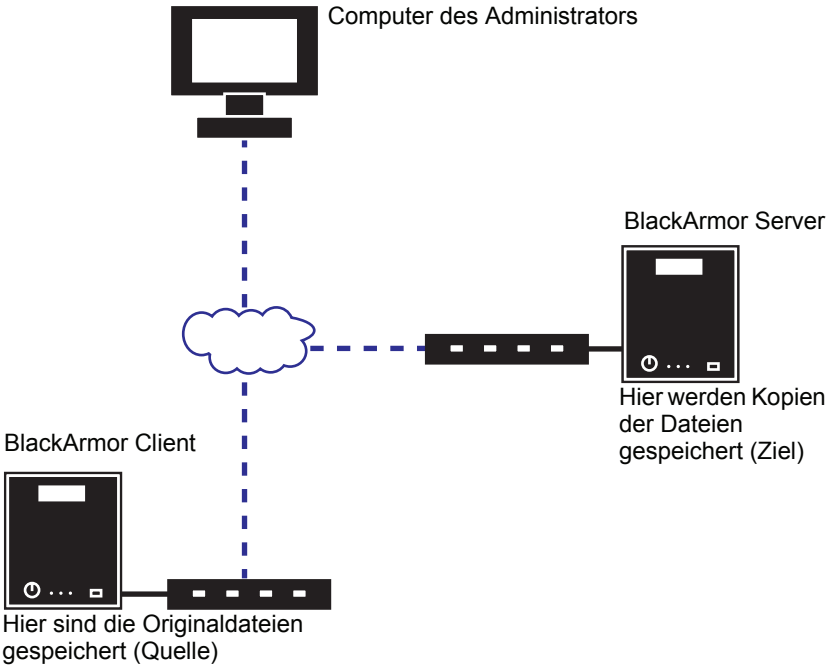
Wenn Sie die Zugriffsberechtigungen für die Freigaben auf dem BlackArmor-Server bearbeiten, können Sie eine ganze Gruppe einer Zugriffsstufe zuordnen, anstatt jeden Benutzer einzeln zuzuordnen.

Zum Erstellen, Ändern oder Löschen einer Benutzergruppe rufen Sie BlackArmor Manager auf (siehe Seite 16). Gruppen finden Sie im Menü „Zugriff“. Schrittweise Anleitungen zur Verwendung von BlackArmor Manager finden Sie in der Onlinehilfe.

Netzwerksicherung der Dateien auf dem BlackArmor-Server

Der BlackArmor-Server verfügt über zwei LAN-Anschlüsse, von denen einer für die Verbindung des Servers mit dem lokalen Netzwerk verwendet werden muss (normalerweise Anschluss 1). Die beiden LAN-Anschlüsse des Servers können für *Link Aggregation* konfiguriert werden. Dabei werden beide LAN-Anschlüsse gleichzeitig für die Verbindung zum Netzwerk verwendet. Dies ermöglicht einen sogenannten Failover-Schutz, d. h., die zweite Verbindung (Port) übernimmt, wenn die erste ausfällt. Siehe Seite 39.

Alternativ können Sie die NAS-zu-NAS-Sicherung einrichten, bei der eine ständige Verbindung zwischen dem BlackArmor-Server und einem anderen Server im Netzwerk hergestellt wird, über die automatisch eine fortlaufende Sicherung der Daten auf dem BlackArmor-Server durchgeführt wird. Die fortlaufende Datensicherung bietet den besten Schutz gegen Datenverlust und Geräteausfall, vor allem wenn der zweite Server sich in einem anderen Gebäude oder einem anderen Teil der Stadt (oder des Landes) befindet als der BlackArmor-Server.



Richten Sie mit BlackArmor Manager eine Netzwerkverbindung zwischen den beiden Servern – dem BlackArmor-Client, auf dem die Dateien der BlackArmor-Benutzer gespeichert sind, und dem BlackArmor-Server, auf dem die Kopien der Dateien gespeichert werden – ein und starten Sie die erste Sicherung. Anschließend richten Sie mit BlackArmor Manager regelmäßige Sicherungen ein.

Bevor Sie Daten vom BlackArmor®-Server auf einen anderen Server im Netzwerk sichern können, müssen Sie den Sicherungsdienst aktivieren.

1. Starten Sie BlackArmor Manager (siehe Seite 16).
2. Klicken Sie in der Menüleiste auf **Speicher** und dann auf **Sicherungsmanager**.
3. Klicken Sie links im Fenster im Menü **Speicher** auf **Servereinstellungen**.
4. Aktivieren Sie das Kontrollkästchen neben **Sicherungsdienst**.

Die Authentifizierungsdaten werden angezeigt. Diese werden bei der Wiederherstellung gesicherter Dateien verwendet.

5. Geben Sie einen Namen und ein Kennwort zur Authentifizierung für alle Aliasse ein.
6. Wählen Sie den Datenträger für die Speicherung aus.
7. Geben Sie einen Aliasnamen ein und klicken Sie dann auf **Neuen Alias hinzufügen**.
8. Klicken Sie auf **Senden**.

Die Einstellungen werden gespeichert.

9. Weitere Informationen über die Sicherungsaufgaben, die Sie einrichten können, finden Sie in der Onlinehilfe von BlackArmor Manager.

Einrichten der Link Aggregation

Die beiden LAN-Anschlüsse des Servers können für *Link Aggregation* konfiguriert werden. Dabei werden beide LAN-Anschlüsse gleichzeitig für die Verbindung zum Netzwerk verwendet. Dies ermöglicht einen sogenannten Failover-Schutz, d. h., die zweite Verbindung (Port) übernimmt, wenn die erste ausfällt. Siehe Seite 39.

Zur Einrichtung der Link Aggregation verbinden Sie beide LAN-Anschlüsse des BlackArmor-Servers durch Ethernetkabel mit dem Netzwerk-Switch oder -Router. Rufen Sie anschließend BlackArmor Manager auf (siehe Seite 16) und wählen Sie die LAN-Einstellung **Aggregation** aus. Die LAN-Einstellungen finden Sie im Menü „Netzwerk“. Schrittweise Anleitungen zur Verwendung von BlackArmor Manager finden Sie in der Onlinehilfe.

Einrichten des BlackArmor-Servers als Media Server

Sie können Fotos, Videos und Musik auf dem BlackArmor-Server speichern und für jeden verfügbar machen.

Mit BlackArmor Manager können Sie den Server als Media Server einrichten und Mediendateien automatisch in festgelegte Ordner herunterladen lassen. Zum Beispiel könnten alle Musikdateien, die ein Benutzer herunterlädt, im Ordner „Musik“ des jeweiligen Benutzers abgelegt werden.

Sie können den BlackArmor-Server auch als iTunes-Server einrichten, um den BlackArmor-Benutzern das Streaming von Musik zu einem Netzwerkcomputer mit iTunes-Software oder einem iPod, der an einen Netzwerkcomputer angeschlossen ist, zu ermöglichen.

Zur Einrichtung des BlackArmor-Servers als Media Server rufen Sie BlackArmor Manager auf (siehe Seite 16) und gehen Sie zum Menü „Medien“. Schrittweise Anleitungen zur Verwendung von BlackArmor Manager finden Sie in der Onlinehilfe.

Überwachen des BlackArmor-Servers

BlackArmor Manager und der BlackArmor-Server selbst bieten verschiedene Möglichkeiten, Aktivität und Status des Servers zu überwachen:

- Überwachen des Status anhand der LCD-Anzeige des Servers
- Überwachen des Status anhand der LED-Anzeigen des Servers
- Verwenden von E-Mail-Benachrichtigungen über den Serverstatus
- Überprüfen des Festplattenstatus mit SMART

Überwachen des Status anhand der LCD-Anzeige des Servers

An der Vorderseite des BlackArmor-Servers befindet sich eine LCD-Anzeige, auf der Informationen zu Einstellungen und Status des Servers angezeigt werden.

Mit den Navigationstasten neben der Anzeige können Sie die verfügbaren Informationen abrufen. Halten Sie nach Auswahl eines Elements die Taste gedrückt, um weitere Einzelheiten anzuzeigen.

Bei einem „Ereignis“ auf dem Server – etwa wenn Sie eine Einstellung ändern oder ein Fehler (Unterbrechung der Netzwerkverbindung, Ausfall einer Festplatte usw.) auftritt – werden Informationen über das Ereignis auf der LCD-Anzeige angezeigt. Bei einem Fehler bleiben die Fehlerinformationen auf der Anzeige, bis das Problem behoben ist.

Überwachen des Status anhand der LED-Anzeigen des Servers

Der BlackArmor-Server besitzt acht LED-Anzeigen, über die Sie den Status seiner Komponenten überwachen können. (Zur Anordnung der LED-Anzeigen siehe die Abbildung auf Seite 9.)

Tabelle 2: LED-Anzeigen an der Vorder- und Rückseite

LED-Anzeige	Status und Farbe	Bedeutung
Betrieb	Leuchtet blau	Der Server ist eingeschaltet.
	Aus	Der Server ist ausgeschaltet.
Systemstatus	Leuchtet blau	Der Server ist betriebsbereit.
	Leuchtet gelb	Beim Server ist ein Systemfehler aufgetreten.
LAN-Anschluss 1	Aus	Der Anschluss hat keine Netzwerkverbindung.
	Leuchtet blau	Der Anschluss hat eine Netzwerkverbindung.
	Blinkt blau	Es werden Daten übertragen.
LAN-Anschluss 2	Aus	Der Anschluss hat keine Netzwerkverbindung.
	Leuchtet blau	Der Anschluss hat eine Netzwerkverbindung.
	Blinkt blau	Es werden Daten übertragen.
Festplatte 1	Leuchtet blau	Die Festplatte ist installiert und arbeitet ordnungsgemäß.
	Leuchtet gelb	Die Festplatte wurde entfernt oder ist defekt.
Festplatte 2	Leuchtet blau	Die Festplatte ist installiert und arbeitet ordnungsgemäß.
	Leuchtet gelb	Die Festplatte wurde entfernt oder ist defekt.
Festplatte 3	Leuchtet blau	Die Festplatte ist installiert und arbeitet ordnungsgemäß.
	Leuchtet gelb	Die Festplatte wurde entfernt oder ist defekt.
Festplatte 4	Leuchtet blau	Die Festplatte ist installiert und arbeitet ordnungsgemäß.
	Leuchtet gelb	Die Festplatte wurde entfernt oder ist defekt.

Verwenden der LED-Anzeigen zur Überwachung des Servers

1. Die Systemstatus-LED zeigt an, ob ein Problem vorliegt. Wenn sie blau leuchtet, arbeiten der Server und seine Komponenten ordnungsgemäß.

Leuchtet sie gelb, ist ein Problem aufgetreten.

2. Überprüfen Sie die LAN-LEDs an der Rückseite des Servers und die Festplatten-LEDs hinter der Tür, um die Fehlerursache einzugrenzen.
3. Falls eine oder beide LAN-LEDs nicht leuchten, könnte die Netzwerkverbindung unterbrochen sein. Falls eine Festplatten-LED gelb leuchtet, ist die Festplatte möglicherweise defekt (oder wurde entfernt).

Siehe Kapitel 6 „Beheben von Problemen“ auf Seite 53 zur Behebung des Problems.

Verwenden von E-Mail-Benachrichtigungen über den Serverstatus

Hinweis: E-Mail-Benachrichtigungen können nur von BlackArmor-Administratoren eingerichtet werden.

Sie können in BlackArmor Manager einrichten, dass Sie per E-Mail benachrichtigt werden, wenn der Status des Servers sich ändert oder eine Servereinstellung geändert wird. BlackArmor Manager kann E-Mail-Benachrichtigungen an bis zu fünf Empfänger versenden. Zum Empfang von Benachrichtigungen benötigen Sie ein Seagate Global Access-Konto.

Zur Einrichtung von E-Mail-Benachrichtigungen rufen Sie BlackArmor Manager auf (siehe Seite 16). E-Mail-Benachrichtigungen finden Sie im Menü „System“. Schrittweise Anleitungen zur Verwendung von BlackArmor Manager finden Sie in der Onlinehilfe.

Überprüfen des Festplattenstatus mit SMART

Hinweis: Die SMART-Diagnose kann nur von BlackArmor-Administratoren durchgeführt werden.

Mit BlackArmor Manager können Sie SMART-Diagnosen für die Festplatten im Server durchführen.

SMART steht für Self-Monitoring Analysis and Reporting Technology (System zur Selbstüberwachung, Analyse und Statusmeldung). Dabei handelt es sich um ein in Festplatten integriertes System, mit dem diese ihren eigenen Systemzustand überwachen und mögliche Probleme melden können.

Durch die regelmäßige Ausführung einer SMART-Diagnose für die Festplatten des Servers kann Festplattenausfällen vorgebeugt werden, da dabei Probleme frühzeitig erkannt werden. Da nur Festplatten mit SMART-Unterstützung mit BlackArmor Manager geprüft werden können, sollten Sie stets nur SMART-Festplatten im Server verwenden.

Zur Ausführung einer SMART-Diagnose rufen Sie BlackArmor Manager auf (siehe Seite 16). Die SMART-Tests finden Sie im Menü „System“. Schrittweise Anleitungen zur Verwendung von BlackArmor Manager finden Sie in der Onlinehilfe.

Ändern der erweiterten Einstellungen des BlackArmor-Servers

Dieser Abschnitt beschreibt einige der Servereinstellungen, die Sie möglicherweise Ihren Bedürfnissen entsprechend ändern möchten.

Hinweis: Einige Einstellungen sollten nur von Personen mit gründlichen Kenntnissen der entsprechenden Technologien geändert werden. Diese sind entsprechend gekennzeichnet.

Dieser Abschnitt behandelt folgende Themen:

- DDNS-Einstellungen
- Dateiprotokolleinstellungen
- NTP-Einstellungen
- Energiespareinstellungen
- SSL-Einstellungen
- USV-Einstellungen
- Internet-Protokoll-Einstellungen
- Arbeitsgruppen- und Domäneneinstellungen

DDNS-Einstellungen

Hinweis: Diese Einstellungen sollten nur von Personen geändert werden, die mit Dynamic DNS vertraut sind.

DDNS (Dynamic DNS) ist ein System, das eine Verbindung zwischen einem unveränderlichen Domänennamen (wie www.seagate.com) und den sich ständig ändernden IP-Adressen eines Computers, der statt einer statischen IP-Adresse DHCP verwendet, herstellt. Ein DDNS-Dienst verfolgt sich ändernde IP-Adressen und leitet den Datenverkehr für Ihren Domänennamen an die jeweils gültige IP-Adresse weiter.

Sie können Dynamic DNS für den BlackArmor-Server mit BlackArmor Manager einrichten. In BlackArmor Manager müssen Sie einen DDNS-Anbieter auswählen und einen Domänennamen für den Server angeben. Weitere Informationen erhalten Sie auf der Website des gewählten DNS-Anbieters.

Zur Einrichtung von DDNS rufen Sie BlackArmor Manager auf (siehe Seite 16). Dynamic DNS finden Sie im Menü „Netzwerk“. Schrittweise Anleitungen zur Verwendung von BlackArmor Manager finden Sie in der Onlinehilfe.

Dateiprotokolleinstellungen

Zur gemeinsamen Nutzung von Dateien auf verschiedenen Computern in einem Netzwerk werden standardisierte Dateidienste verwendet. Informationen über die unterstützten Protokolle finden Sie unter „Besondere Funktionen für Freigaben“ auf Seite 34.

NTP-Einstellungen

Ein NTP-Zeitserver (Network Time Protocol – Netzwerkzeitprotokoll) sorgt für die Synchronisierung von Datum und Uhrzeit des BlackArmor-Servers. NTP läuft ständig und gleicht die Zeit des BlackArmor-Servers mit der Uhr des NTP-Zeitservers ab.

Sie können den NTP-Dienst auf dem BlackArmor-Server aktivieren, indem Sie die vollständige Domänenbezeichnung (FQDN, Fully Qualified Domain Name) oder IP-Adresse des NTP-Zeitservers angeben. Zum Einrichten des NTP-Dienstes öffnen Sie BlackArmor Manager und wählen Sie im Menü „System“ die Option **Allgemeine Einrichtung**. Weitere Informationen finden Sie in der Onlinehilfe.

Energiespareinstellungen

Normalerweise drehen sich die Festplatten im BlackArmor-Server ununterbrochen, wenn der Server eingeschaltet ist, auch wenn dieser gar nicht genutzt wird, wie zum Beispiel abends, am Wochenende oder an Feiertagen.

Mit der Energiesparfunktion von BlackArmor Manager können Sie dafür sorgen, dass die Festplatten bei Inaktivität *heruntergefahren* (angehalten) und in den Standby-Modus versetzt werden, um Energie – und Stromkosten – zu sparen. Den Energiesparmodus aktivieren Sie auf der Seite **Erweitert** im Menü „System“.

SSL-Einstellungen

Hinweis: Die SSL-Unterstützung sollte auf dem BlackArmor-Server nur von Personen eingerichtet werden, die mit SSL vertraut sind.

SSL (oder Transportschicht-Sicherheit) ist ein Verschlüsselungsverfahren, das zum Schutz von Daten bei der Übertragung über ein Netzwerk oder das Internet verwendet wird. Dabei wird ein System aus Schlüsseln, wie geheimen Kennwörtern, verwendet, um Dateien sicher zu versenden und zu empfangen. Weitere Informationen finden Sie unter „Internet-Protokoll-Einstellungen“ auf Seite 44.

Sie können die SSL-Unterstützung auf dem BlackArmor-Server einrichten, indem Sie ein SSL-Zertifikat und ein Schlüsselpaar eingeben.

USV-Einstellungen

Eine USV (unterbrechungsfreie Stromversorgung) ist mit einem Akku ausgestattet, um bei Stromausfällen die Stromversorgung zu einem Computer oder Server aufrechtzuerhalten.

USV sind darauf ausgelegt, die Stromversorgung lange genug zu gewährleisten, um geöffnete Dateien zu speichern und das System ordnungsgemäß herunterzufahren. Sie sind nicht dazu gedacht, das System für die Dauer des Stromausfalls am Laufen zu halten.

Sie können den BlackArmor-Server an eine USV anschließen und die USV-Einstellungen in BlackArmor Manager anpassen. Dabei können Sie festlegen, wann die USV den BlackArmor-Server herunterfahren soll, falls Sie nicht vor Ort sind. Dabei können Sie zwischen folgenden Möglichkeiten wählen:

- Der Server wird heruntergefahren, wenn die verbleibende Akkuleistung der USV auf 15 % oder weniger als 5 Minuten gesunken ist.

oder

- Der Server wird heruntergefahren, wenn nach Beginn des Stromausfalls eine gewisse Zeit verstrichen ist. (Sie können diesen Zeitraum festlegen.)

Internet-Protokoll-Einstellungen

Standardmäßig ist der BlackArmor-Server auf das Internet-Protokoll HTTP eingestellt. HTTP steht für Hypertext Transfer Protocol (Hypertext-Übertragungsprotokoll), das Protokoll, das am häufigsten für den Austausch von Daten und Dateien im Internet verwendet wird.

Wenn Sie SSL aktiviert haben, können Sie den BlackArmor-Server auf die Verwendung von HTTPS (HTTP over Secure Socket Layer – sicheres Hypertext-Übertragungsprotokoll) einstellen. (Siehe „SSL-Einstellungen“ auf Seite 43.)

Arbeitsgruppen- und Domäneneinstellungen

Standardmäßig ist der BlackArmor-Server als *Arbeitsgruppe* eingerichtet. Eine Arbeitsgruppe ist eine Gruppe von Computern in einem Netzwerk, die Ressourcen gemeinsam nutzen. Sie können beliebige Computer zur Arbeitsgruppe des Servers hinzufügen oder den Server zu einer bestehenden Arbeitsgruppe hinzufügen.

Sie können den BlackArmor-Server aber auch zum Mitglied einer *Domäne* machen. Eine Domäne ist eine Gruppe von Computern, die als Einheit zentral verwaltet werden.

Wenn Sie den BlackArmor-Server als Mitglied einer Domäne hinzufügen, wird er von einem Windows-Domänencontroller zentral verwaltet. Dies bietet zusätzliche Sicherheit beim Zugriff von Benutzern auf den Server. Benutzer in der Domäne erhalten ein eigenes Konto und müssen authentifiziert werden, um auf den Server zuzugreifen.

Nur der Domänenadministrator kann den BlackArmor-Server zum Mitglied einer Domäne machen. Damit Sie den Server zu einer Domäne hinzufügen können, müssen Sie den Benutzernamen und das Kennwort des Domänenadministrators kennen. Eine Anleitung dazu, wie Sie den Server als Mitglied einer Domäne hinzufügen, finden Sie in der Onlinehilfe von BlackArmor Manager.

Warten des BlackArmor-Servers

Dieser Abschnitt beschreibt die grundlegenden Aufgaben, mit denen Sie den reibungslosen Betrieb des BlackArmor-Servers gewährleisten können.

Dieser Abschnitt behandelt folgende Themen:

- „Hinweise zu Sicherheit und Wartung der Hardware“ auf Seite 45
- „Aktualisieren der Server-Firmware“ auf Seite 46
- „Zurücksetzen des BlackArmor-Servers“ auf Seite 46

Hinweise zu Sicherheit und Wartung der Hardware

Beachten Sie folgende Punkte, um den reibungslosen Betrieb des BlackArmor-Servers zu gewährleisten. Nichtbeachtung kann zu Leistungsbeeinträchtigungen und Datenverlust führen.

- Verwenden Sie immer BlackArmor Manager oder den Netzschalter an der Vorderseite, um den Server herunterzufahren und neu zu starten (eine Anleitung finden Sie in der Onlinehilfe von BlackArmor Manager). Sie sollten niemals einfach den Netzstecker ausstecken oder die Steckdose ausschalten.
- Stellen Sie den Server auf eine stabile und ebene Oberfläche. Halten Sie den Server kühl und trocken. Achten sie darauf, dass die Lüftungsschlitze nicht blockiert sind, um eine Überhitzung zu vermeiden.
- Reinigen Sie das Servergehäuse nur von außen mit einem feuchten Tuch (verwenden Sie keine Reinigungsmittel) und stecken Sie vor dem Reinigen den Netzstecker aus, um Stromschläge zu vermeiden.
- Versuchen Sie nicht, das Gehäuse des Servers zu öffnen oder abzunehmen. Sie können Festplatten entfernen und austauschen, aber versuchen Sie nicht, andere Wartungsarbeiten an der Hardware vorzunehmen.
- Entfernen Sie niemals mehr als eine Festplatte gleichzeitig. Dies kann zu Datenverlust führen.
- Wenden Sie sich in den folgenden Fällen an den Kundendienst:
  - Wenn das Netzkabel des Servers beschädigt ist
  - Wenn Flüssigkeit auf den Server verschüttet wurde oder der Server mit Wasser in Berührung gekommen ist
  - Wenn der Server heruntergefallen ist oder das Gehäuse beschädigt ist
  - Wenn der Server nicht normal arbeitet, obwohl Sie alle Betriebsanweisungen beachtet haben

Aktualisieren der Server-Firmware

Hinweis: Die Firmware des Servers kann nur von BlackArmor-Administratoren aktualisiert werden.

Sie sollten die *Firmware* des Servers (in den Server integrierte Software) aktualisieren, wenn neue Versionen verfügbar sind, sodass die Funktionen immer auf dem neuesten Stand sind. Neue Versionen der BlackArmor-Firmware finden Sie auf der Seagate-Website unter www.seagate.com.

In BlackArmor Manager können Sie zwischen zwei Aktualisierungsverfahren wählen:

- **Automatische Firmware-Updates**: BlackArmor Manager lädt neue Firmware-Versionen herunter, führt die Aktualisierung durch und startet den Server neu. Sie können die Aktualisierung sofort starten oder einen geeigneten Zeitpunkt für die Aktualisierung festlegen.

Sie können auch einstellen, dass BlackArmor Manager regelmäßig nach neuen Versionen der Firmware sucht und entweder meldet, wenn eine neue Version verfügbar ist, oder das Update automatisch aktualisiert.

- **Manuelle Firmware-Updates**: Sie müssen auf der Seagate-Website unter www.seagate.com nachsehen, ob eine neue Firmware-Version verfügbar ist, die Firmware-Dateien selbst herunterladen und die Aktualisierung starten.

Seagate empfiehlt die Verwendung automatischer Updates, um zu gewährleisten, dass der Server stets die neueste, stabilste Version der BlackArmor-Firmware verwendet.

Zurücksetzen des BlackArmor-Servers

Führen Sie die folgenden Schritte aus, um den Servernamen, die DHCP-Einstellung (Netzwerkmodus) und das Kennwort für die Anmeldung beim Server zurückzusetzen.

Hinweis: Für diesen Vorgang benötigen Sie eine Büroklammer oder einen anderen spitzen Gegenstand.

1. Verschaffen Sie sich Zugang zur Rückseite des Servers.
2. Vergewissern Sie sich, dass der Server eingeschaltet und an das LAN angeschlossen ist.
3. An der Rückseite des Servers befindet sich eine kleine Öffnung, in der die Reset-Taste sitzt.
4. Stecken Sie ein Ende der Büroklammer in die Öffnung, drücken Sie die Reset-Taste und halten Sie sie gedrückt. Lassen Sie die Taste noch *nicht* los.
5. Halten Sie die Reset-Taste gedrückt, bis die Festplatten-LEDs an der Vorderseite des Servers aufleuchten und auf gelb springen. Dies dauert einige Sekunden.
6. Lassen Sie die Reset-Taste los.

Der Server startet neu. Wenn der Server neu gestartet ist und die LAN- und Festplatten-LEDs leuchten, ist der Server zurückgesetzt. Der Servername wird auf „BA-*MAC-Adresse*“ zurückgesetzt (*MAC-Adresse* entspricht den letzten sechs Zeichen der MAC-Adresse des Servers).

5. Tipps für BlackArmor®-Benutzer

- Einführung
- Informationen zum BlackArmor-Benutzerkonto
- Zugreifen auf Freigaben und Dateien auf dem BlackArmor-Server
- Sichern von Dateien
- Zugreifen auf BlackArmor-Dateien über das Internet
- Herunterladen großer Dateien aus dem Internet auf den BlackArmor-Server
- Wiederherstellen gelöschter Dateien im Papierkorb

Einführung

In diesem Kapitel finden BlackArmor®-Benutzer Tipps und Informationen zur optimalen Nutzung des BlackArmor-Servers.

BlackArmor-Benutzer können folgende Funktionen nutzen:

- Speichern und Freigeben von Dateien auf dem BlackArmor Server
- Sichern von Dateien, Anwendungen und sogar Betriebssystemen mit BlackArmor Backup
- Zugriff auf den BlackArmor-Server über das Internet durch Global Access (falls aktiviert)
- Herunterladen großer Dateien aus dem Internet direkt auf den BlackArmor-Server mit dem Download-Tool von BlackArmor Manager
- Wiederherstellen versehentlich gelöschter Dateien aus dem BlackArmor Manager-Papierkorb (falls aktiviert)

Informationen zum BlackArmor-Benutzerkonto

Dieser Abschnitt beschreibt die Merkmale und möglichen Einschränkungen Ihres BlackArmor-Benutzerkontos.

Zugriffseinschränkungen

Freigaben auf dem BlackArmor-Server können öffentlich (mit gewissen Einschränkungen für jeden zugänglich) oder privat (auf bestimmte Benutzerkonten beschränkt) sein.

Fragen Sie Ihren BlackArmor-Administrator, welche Zugriffseinschränkungen für Sie gelten.

Private Freigaben

Private Freigaben sind durch ein Kennwort geschützt und können nur durch die vom BlackArmor-Administrator festgelegten Personen genutzt werden.

Wenn der BlackArmor-Administrator ein Benutzerkonto eingerichtet hat, können Sie den Zugriff auf eine private Freigabe wie folgt einschränken:

- Einschränkung des Zugriffs auf bestimmte BlackArmor-Benutzer
- Einschränkung bestimmter BlackArmor-Benutzer auf reinen Lesezugriff. Bei *Lesezugriff* kann der Benutzer die Dateien in der Freigabe anzeigen, aber keine Dateien bearbeiten oder in der Freigabe speichern.

Sie haben vollen Zugriff auf Ihre private Freigabe. Damit können Sie ihre Dateien in der Freigabe speichern und sichern sowie Dateien in der Freigabe bearbeiten und auf Ihren Computer oder ein an den Server angeschlossenes USB-Laufwerk herunterladen (siehe Seite 51).

Sie können anderen Benutzern mit Global Access lokalen oder Fernzugriff auf einzelne oder alle Dateien in Ihrer privaten Freigabe geben. Weitere Informationen und eine Anleitung zur Einrichtung eines Global Access-Kontos finden Sie auf Seite 25. Einzelheiten dazu, wie Sie anderen Personen Zugriff auf Ihre private Freigabe geben können, finden Sie in der Dokumentation zu Global Access.

Hinweis: Wenn mehrere *private* Freigaben gleichzeitig verbunden werden sollen, müssen diese dieselben Authentifizierungsdaten besitzen.

Öffentliche Freigaben

Öffentliche Freigaben unterliegen keinen Einschränkungen. Sie können beliebig viele öffentliche Freigaben verbinden.

Speicherplatzeinschränkungen

Ihr BlackArmor-Administrator kann den Speicherplatz einschränken, den Sie bei einer bestimmten Freigabe beanspruchen dürfen.

Es kann sein, dass Ihr Speicherplatz bei einer Freigabe eingeschränkt ist und bei einer anderen nicht, oder dass Ihnen bei einer Freigabe mehr Platz zur Verfügung steht als bei einer anderen. Möglicherweise gelten für Sie auch keine Speicherplatzeinschränkungen (abgesehen von der Kapazität des BlackArmor-Servers selbst).

Fragen Sie Ihren BlackArmor-Administrator, ob und welche Speicherplatzeinschränkungen für Sie gelten.

Wenn Sie die Grenzen des Ihnen zugeteilten Speicherplatzes erreicht haben, löschen Sie entweder nicht mehr benötigte Dateien oder bitten Sie Ihren BlackArmor-Administrator, Ihnen mehr Speicherplatz zuzuteilen.

Automatische Sortierung von Mediendateien

Für Freigaben auf dem BlackArmor-Server kann eingerichtet werden, dass Mediendateien je nach Dateityp automatisch in bestimmte Ordner auf Ihrem Computer sortiert werden. Wenn Sie zum Beispiel Musikdateien herunterladen, würden diese dann automatisch im Ordner „Gemeinsame Musik“ abgelegt werden.

Fragen Sie Ihren BlackArmor-Administrator, ob für die Freigaben, auf die Sie Zugriff haben, die automatische Sortierung (in BlackArmor Manager als „Drag&Sort“ bezeichnet) eingerichtet ist.

Kulanzzeiten für Kontingente

Falls für Ihr Konto ein Speicherplatzkontingent festgelegt wurde, kann der BlackArmor-Administrator eine Kulanzzeit einstellen, in der das Kontingent vorübergehend überschritten werden darf. Nach der Kulanzzeit können keine weiteren Dateien mehr gespeichert werden, bis wieder Platz verfügbar gemacht wird.

Fragen Sie Ihren BlackArmor-Administrator, ob für den Server Kulanzzeiten für gespeicherte Dateien festgelegt wurden.

Unterstützung für Dateiprotokolle

Für den Zugriff auf Dateien durch Computer in einem Netzwerk werden standardisierte Dateiprotokolle verwendet. Informationen über die unterstützten Protokolle finden Sie unter Besondere Funktionen für Freigaben.

Zugreifen auf Freigaben und Dateien auf dem BlackArmor-Server

Nachdem Sie die Verbindung zum BlackArmor-Server hergestellt und die Freigaben, auf die Sie Zugriff haben, verbunden haben, können Sie unmittelbar Dateien auf dem Server speichern.

Hinweis: Sie können beliebig viele öffentliche und private Freigaben verbinden. Wenn mehrere *private* Freigaben verbunden werden sollen, müssen diese jedoch dieselben Authentifizierungsdaten besitzen.

Sie können auf verschiedene Arten auf die Freigaben auf dem BlackArmor-Server zugreifen:

- Lokal, so wie Sie auf ein Netzlaufwerk auf Ihrem Computer zugreifen (z. B. mit Windows Explorer). Auf Seite 24 wird beschrieben, wie Sie Freigaben mit Ihrem Computer verbinden können.
- Über das Internet durch Seagate Global Access (falls Ihr BlackArmor-Administrator Global Access auf dem BlackArmor-Server aktiviert hat). Weitere Informationen über Global Access finden Sie auf Seite 25.

Wenn Sie Zugriff auf eine Freigabe haben, können Sie entsprechend Ihren Berechtigungen Dateien in der Freigabe anzeigen und herunterladen sowie Dateien in die Freigabe hochladen und sichern (siehe Seite 47).

Informationen über den Zugriff auf die Freigaben, die Sie benötigen, und über Ihre Berechtigungen für das Anzeigen, Herunterladen und Hochladen von Dateien erhalten Sie von Ihrem BlackArmor-Administrator.

Sichern von Dateien

Sichern Sie wichtige Dateien regelmäßig mit BlackArmor Backup, um sie gegen Verlust, Beschädigung und versehentliches Löschen zu schützen.

Sie können auch Dateien vom BlackArmor-Server auf ein externes USB-Laufwerk oder von einem USB-Laufwerk auf den Server sichern.

Sichern von Dateien mit BlackArmor Backup

BlackArmor Backup ist eine vollständige Sicherungssoftware mit vielfältigen Optionen, mit der Sie das passende Sicherungssystem für Ihre Bedürfnisse einrichten können.

Sie können mit BlackArmor Backup jederzeit eine Sicherung starten. Außerdem können Sie mit BlackArmor Backup regelmäßige Sicherungen einrichten, die zu einem geeigneten Zeitpunkt ausgeführt werden (z. B. nachts oder am Wochenende, wenn Sie den Computer nicht benutzen).

Mit BlackArmor Backup können Sie alle Dateien, Anwendungen und sogar das Betriebssystem auf Ihrem Computer sichern.

Falls Sie BlackArmor Backup noch nicht installiert haben, finden Sie auf Seite 24 eine Installationsanleitung.

Weitere Informationen finden Sie im *BlackArmor Backup-Benutzerhandbuch* oder in der Onlinehilfe.

Sichern von Server zu Server

Hinweis: Diese Aufgabe kann nur von Administratoren ausgeführt werden.

Sie können mit BlackArmor Manager Daten vom BlackArmor-Server auf einen anderen Server im Netzwerk sichern und umgekehrt. Zur Sicherung auf einen anderen Server benötigen Sie dessen IP-Adresse und Authentifizierungsdaten.

Den Sicherungsmanager finden Sie in BlackArmor Manager im Menü „Speicher“. Eine schrittweise Anleitung zur Sicherung von Server auf Server finden Sie in der Onlinehilfe von BlackArmor Manager.

Sichern von oder auf externe USB-Laufwerke

Hinweis: Die folgenden Schritte können nur von Administratoren ausgeführt werden.

Mit BlackArmor Manager können Sie Ihre Dateien sofort (oder zu einem festgelegten Zeitpunkt) *von* einem externen USB-Laufwerk *auf* den BlackArmor-Server oder *vom* BlackArmor-Server auf ein externes USB-Laufwerk sichern.

Zur Sicherung von einem oder auf ein externes USB-Laufwerk schließen Sie das USB-Laufwerk an einen freien USB-Anschluss am BlackArmor-Server an (siehe Seite 10) und rufen Sie dann BlackArmor Manager auf (siehe Seite 16). Den Sicherungsmanager finden Sie im Menü „Speicher“.

Eine schrittweise Anleitung zur Sicherung Ihrer Dateien finden Sie in der Onlinehilfe von BlackArmor Manager.

Zugreifen auf BlackArmor-Dateien über das Internet

Falls Ihr BlackArmor-Administrator Global Access auf dem Server aktiviert hat, richten Sie ein kostenloses Global Access-Konto ein, damit Sie über das Internet auf die Dateien auf dem BlackArmor-Server zugreifen können.

Seagate Global Access ist ein Service, über den Sie die Dateien auf dem BlackArmor-Server von jedem Ort aus anzeigen, herunterladen und bearbeiten können, Dateien in einer privaten Freigabe verfügbar machen können und Dateien für Personen außerhalb Ihres Netzwerks freigeben können.

Global Access bietet Ihnen folgende Möglichkeiten:

- Sie können wichtige geschäftliche Dateien oder Präsentationen vom Büro eines Kunden aus an jedem Ort der Welt herunterladen.
- Sie können Dateien für Kunden verfügbar machen, ohne dass diese eine FTP-Anwendung verwenden müssen.
- Sie können wichtige Dateien von Ihrem Notebook hochladen und sicher geschützt wissen, während Sie weiterreisen.
- Sie können anderen Personen Zugriff auf die Dateien in Ihrer privaten Freigabe geben.

Damit Sie über das Internet auf den BlackArmor-Server zugreifen können:

- Vergewissern Sie sich, dass Global Access auf dem BlackArmor-Server aktiviert ist. Fragen Sie Ihren BlackArmor-Administrator danach.
- Richten Sie ein Global Access-Konto ein. Jeder Benutzer, der über das Internet auf den BlackArmor-Server zugreifen möchte, braucht ein eigenes Global Access-Konto. (Das Konto ist kostenlos.)

Eine Anleitung zur Einrichtung eines Global Access-Kontos finden Sie auf Seite 25. Einzelheiten dazu, wie Sie anderen Personen Zugriff auf Ihre private Freigabe geben können, finden Sie in der Dokumentation zu Global Access.

Herunterladen großer Dateien aus dem Internet auf den BlackArmor-Server

BlackArmor Manager beinhaltet ein spezielles Tool für das Herunterladen großer Dateien von FTP- und anderen Sites im Internet direkt auf den Server. Dieses **Download-Tool** gibt Ihrem BlackArmor-Administrator die Möglichkeit zu steuern, wann große Downloads ausgeführt werden, sodass der Server nicht überlastet wird.

Download-Aufträge werden nicht immer sofort ausgeführt. Internet-Downloads werden in der Reihefolge ausgeführt, in der sie in der Warteschlange des Download-Tools stehen (die von Ihrem BlackArmor-Administrator geändert werden kann). Wenn Ihr Download-Auftrag nicht an erster Stelle steht, wird er nicht sofort ausgeführt.

Zudem kann Ihr BlackArmor-Administrator einschränken, wann Downloads ausgeführt werden und wie viele gleichzeitig stattfinden können (nie mehr als drei). BlackArmor-Administratoren können festlegen, dass Downloads nur abends, am Wochenende oder zu anderen ruhigen Zeiten in der Woche ausgeführt werden.

Wenden Sie sich an Ihren BlackArmor-Administrator, um zu erfahren, wann Sie mit dem Download-Tool Dateien aus dem Internet herunterladen können, oder um einen Download-Auftrag in der Warteschlange nach vorne verschieben zu lassen.

Wiederherstellen gelöschter Dateien im Papierkorb

Die Freigaben auf dem BlackArmor-Server können durch den BlackArmor Manager-Papierkorb geschützt werden. Wenn der Papierkorb für eine Freigabe aktiviert ist, bewahrt BlackArmor Manager Dateien auf, die von der Freigabe gelöscht werden, sodass sie bei Bedarf wiederhergestellt werden können.

Falls Sie eine Datei versehentlich gelöscht haben, rufen Sie BlackArmor Manager auf (siehe Seite 16) und klicken Sie auf **Papierkorb**. Eine schrittweise Anleitung zum Wiederherstellen gelöschter Dateien finden Sie in der Onlinehilfe von BlackArmor Manager.

6. Beheben von Problemen

Dieses Kapitel beschreibt Lösungen für die häufigsten Probleme bei der Einrichtung und Nutzung des BlackArmor®-Servers.

- Allgemeine Tipps zur Problembehebung
- Häufige Probleme und Lösungen
- Austauschen von Festplatten

Allgemeine Tipps zur Problembehebung

Bei Problemen mit der Einrichtung oder Nutzung des BlackArmor-Servers beachten Sie folgende Hinweise:

- Vergewissern Sie sich, dass der Server richtig an das lokale Netzwerk angeschlossen ist. Überprüfen Sie, ob alle Ethernetkabel angeschlossen sind und funktionieren.
- Vergewissern Sie sich, dass das Netzwerk richtig funktioniert.
- Vergewissern Sie sich, dass der Server richtig an die Stromversorgung angeschlossen und eingeschaltet ist. Überprüfen Sie, ob alle Festplatten fehlerfrei funktionieren.
- Vergewissern Sie sich, dass Ihr Computer den Systemanforderungen von BlackArmor entspricht. Weitere Informationen finden Sie unter „Systemanforderungen“ auf Seite 7.
- Vergewissern Sie sich, dass Ihr Computer einen unterstützten Webbrowser verwendet. Informationen über unterstützte Browser finden Sie unter „Systemanforderungen“ auf Seite 7.
- Vergewissern Sie sich, dass Sie sich mit dem richtigen Administratorbenutzernamen und -kennwort anmelden. (Denken Sie daran, dass bei Kennwörtern die Groß-/Kleinschreibung berücksichtigt wird.)

Häufige Probleme und Lösungen

In diesem Abschnitt finden Sie Lösungen zu häufigen Problemen mit BlackArmor Manager.

Die Verbindung zum Server über das lokale Netzwerk kann nicht hergestellt werden.

Vergewissern Sie sich, dass der Server eingeschaltet und an das Netzwerk angeschlossen ist. Vergewissern Sie sich, dass der Server über den LAN-Anschluss 1 mit dem Netzwerk verbunden ist.

Vergewissern Sie sich, dass der Server eingeschaltet und an das Netzwerk angeschlossen ist.

Versuchen Sie von einem anderen Computer aus eine Verbindung zum Server herzustellen.

Verwenden Sie ein anderes Ethernetkabel.

Die Verbindung zum Server über das Internet kann nicht hergestellt werden.

Vergewissern Sie sich, dass am Server Global Access aktiviert ist. Siehe „Einrichten des Zugriffs auf den BlackArmor-Server über Seagate Global Access“ auf Seite 20.

Aktivieren Sie in BlackArmor Manager die E-Mail-Einrichtung und senden Sie eine Test-E-Mail.

BlackArmor Manager kann nicht geöffnet werden.

Vergewissern Sie sich, dass der Server eingeschaltet und an das Netzwerk angeschlossen ist. Starten Sie BlackArmor Discovery und versuchen Sie erneut, eine Verbindung zum Server herzustellen und dann BlackArmor Manager aufzurufen.

Die Anmeldung bei BlackArmor Manager funktioniert nicht.

Vergewissern Sie sich, dass Sie einen gültigen Benutzernamen und ein gültiges Kennwort verwenden. Denken Sie daran, dass bei Benutzernamen und Kennwörtern die Groß-/Kleinschreibung berücksichtigt wird.

Auf eine Freigabe kann nicht zugegriffen werden.

Vergewissern Sie sich, dass Sie zum Zugriff auf die Freigabe berechtigt sind.

Vergewissern Sie sich, dass Sie einen gültigen Benutzernamen und ein gültiges Kennwort verwenden. Denken Sie daran, dass bei Benutzernamen und Kennwörtern die Groß-/Kleinschreibung berücksichtigt wird.

Möglicherweise befindet sich der Datenträger, der die Freigabe enthält, aufgrund eines Festplattenfehlers im eingeschränkten Betrieb. Überprüfen Sie den Status der Festplatten im Server. Weitere Informationen finden Sie unter „Überwachen des Status anhand der LED-Anzeigen des Servers“ auf Seite 40.

Auf eine Datei in einer Freigabe kann nicht zugegriffen werden.

Vergewissern Sie sich, dass Sie zum Zugriff auf die Datei berechtigt sind.

Möglicherweise befindet sich der Datenträger, der die Freigabe enthält, aufgrund eines Festplattenfehlers im eingeschränkten Betrieb. Überprüfen Sie den Status der Festplatten im Server. Weitere Informationen finden Sie unter „Überwachen des Status anhand der LED-Anzeigen des Servers“ auf Seite 40.

In einer Freigabe können keine Dateien mehr gespeichert werden, weil der Datenträger voll ist.

Falls Sie ein Benutzer sind, wenden Sie sich an Ihren BlackArmor-Administrator.

Falls Sie ein Administrator sind, können Sie gegebenenfalls einige der Dateien auf dem Server entfernen.

Die Firmware-Aktualisierung konnte nicht durchgeführt werden.

Versuchen Sie, die Firmware manuell zu aktualisieren. Weitere Unterstützung erhalten Sie vom Seagate-Support unter www.seagate.com/support.

Das Streaming von Musik vom BlackArmor-Server funktioniert nicht.

Vergewissern Sie sich, dass iTunes auf Ihrem Computer installiert ist. Vergewissern Sie sich, dass Ihr Computer an das lokale Netzwerk angeschlossen ist. Vergewissern Sie sich, dass Sie zum Zugriff auf die Freigabe mit den Musikdateien berechtigt sind.

Ein Datenträger befindet sich im eingeschränkten Betrieb.

Möglicherweise ist eine Festplatte ausgefallen. Weitere Unterstützung erhalten Sie vom Seagate-Support unter www.seagate.com/support.

Austauschen von Festplatten

Führen Sie folgende Schritte aus, um eine Festplatte im BlackArmor® NAS 440/420 Server auszutauschen. Gehen Sie analog vor, um eine beschädigte Festplattenhalterung auszutauschen.

Hinweis: Verwenden Sie für den Austausch ausschließlich Seagate-Festplatten. Falls Sie Ersatzteile anderer Hersteller verwenden, erlischt die Garantie des BlackArmor NAS 440/420.

WARNUNG: Vorsichtsmaßnahmen gegen elektrostatische Entladung

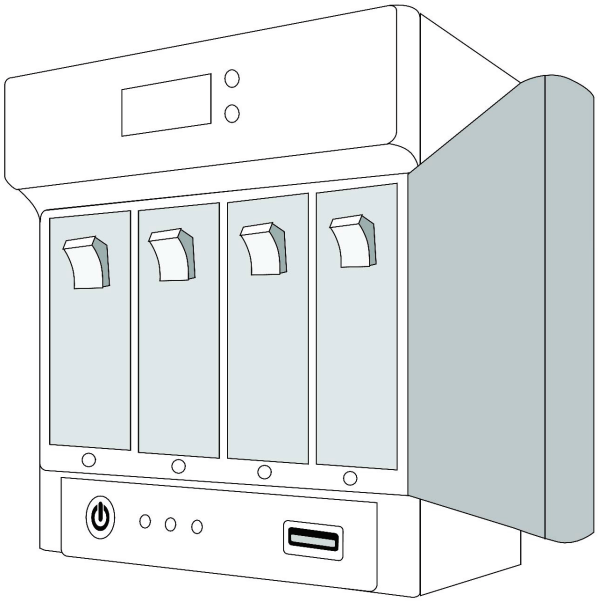
Elektrostatische Entladung kann Prozessor, Festplatten, Mainboard, Speichermodule (RAM) und andere Komponenten des BlackArmor beschädigen. Beachten Sie beim Austausch einer Festplatte folgende Vorsichtsmaßnahmen:

- Lassen Sie die Festplatte bis zum Einbau in der Schutzverpackung.
- Berühren Sie auf keinen Fall Stifte, Drähte oder Platinen der Komponenten.
- Tragen Sie ein Masseband und befestigen Sie es an einem Metallteil des Computergehäuses, bevor Sie Komponenten berühren. Falls kein Masseband verfügbar ist, bleiben Sie bei Vorgängen, die Schutz gegen elektrostatische Entladung erfordern, ständig mit dem Computergehäuse in Kontakt.
- Halten Sie den Arbeitsbereich frei von nicht leitenden Materialien wie Plastikteilen und Schaumstoffverpackungen.

Entfernen einer Festplatte

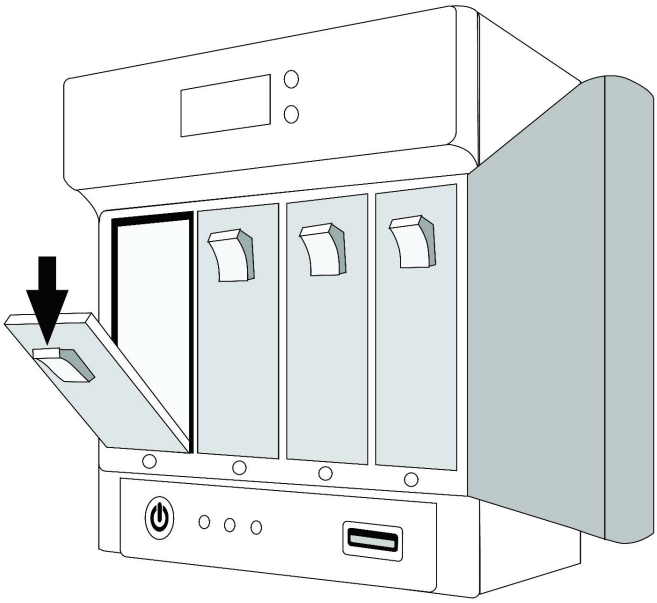
1. Öffnen Sie die Weboberfläche von BlackArmor Manager.
2. Klicken Sie in der Menüleiste auf **Speicher** und dann auf **Datenträgerverwaltung**.
3. Klicken Sie neben der defekten Festplatte auf das Symbol **Festplatte sicher entfernen** und klicken Sie dann auf **OK**.

4. Öffnen Sie die Klappe an der Vorderseite des Servers.



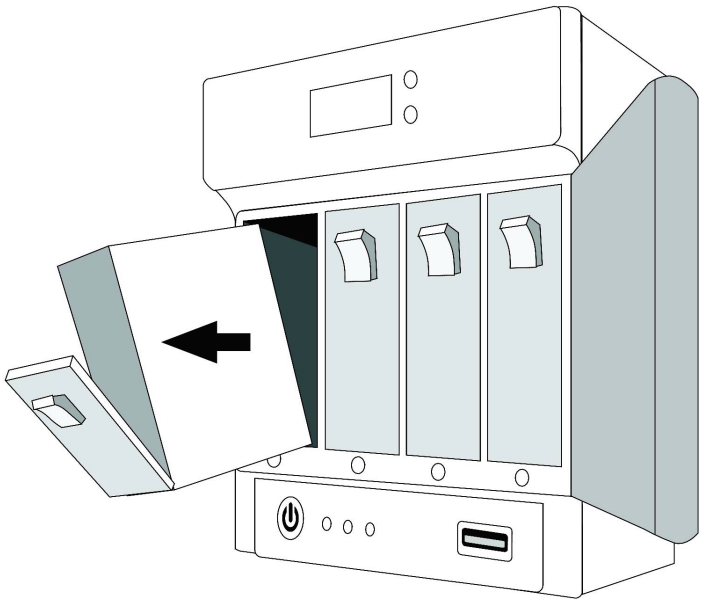
5. Identifizieren Sie die defekte Festplatte. Vergewissern Sie sich, dass auf der Festplatte keine Aktivität stattfindet – die LED der Festplatte sollte nicht leuchten.

Hinweis: Entfernen Sie niemals mehr als eine Festplatte gleichzeitig. Dies kann zu Datenverlust führen.



6. Drücken Sie den orangefarbenen Hebel nach unten, um die defekte Festplatte aus dem Server zu lösen. Falls der Server eingeschaltet ist, warten Sie, bis die Festplatte sich nicht mehr dreht (etwa eine Minute), bevor Sie fortfahren.
7. Ziehen Sie die Festplatte mithilfe des Griffs vorsichtig aus dem Server heraus, bis Sie die Festplatte selbst gut fassen können. Entfernen Sie die Festplatte aus dem Server. Die Festplatte ist schwer – Sie sollten sie nicht am Plastikgriff ganz herausziehen oder am Plastikgriff tragen. Halten Sie die Festplatte an der oberen und unteren Kante fest.

Achtung: **Die Festplatte könnte noch heiß sein, wenn Sie sie ausbauen.**



8. Halten Sie die Festplatte/Halterung so, dass der Festplattenaufkleber nach oben zeigt und der Text lesbar ist (nicht 180° gedreht).
9. Biegen Sie die linke Seite der Plastikhalterung vorsichtig nach außen, um die defekte Festplatte aus der Halterung zu lösen.
10. Nehmen Sie die defekte Festplatte aus der Plastikhalterung.

Austauschen einer Festplatte

1. Legen Sie die neue Festplatte in die Halterung ein. Achten Sie darauf, dass die vier Stifte die Festplatte sicher an Ort und Stelle halten. Wenn Sie eine beschädigte Festplattenhalterung austauschen, bauen Sie die Festplatte aus der beschädigten Halterung aus und setzen Sie sie in die neue Halterung ein.
2. Schieben Sie die neue Festplatte vorsichtig in den Server. Drücken Sie die Halterung fest in den Server und schließen Sie den Griff, um die Festplatte zu arretieren.

Die LED der Festplatte sollte grün aufleuchten.

3. Schließen Sie die Klappe an der Vorderseite des Servers.
4. In BlackArmor Manager ändert sich der Status der Festplatte zu „Fremd“.
5. Klicken Sie auf das Symbol **Festplatte anfordern** und dann auf **OK**.
   Der Festplattenstatus ändert sich zu „Gut“.
6. Klicken Sie auf das Symbol **Wiederherstellen** und dann auf **OK**.

7. Technische Daten

Netzwerkanschluss

- 2 10/100/1000-Ethernet-RJ-45-Anschlüsse

USB-Anschlüsse

- 4 USB-2.0-Anschlüsse (1 an der Vorderseite, 3 an der Rückseite)

Netzteil

- Externes 90-W-Netzteil (für alle Eingangsspannungen geeignet, Ausgangsspannung 19 V)

Festplatten

- 4 SATA-II-Festplatten mit werkzeugfreien Halterungen
- Hot-Swap-fähig

Abmessungen

- Höhe: 200 mm
- Breite: 160 mm
- Tiefe: 210 mm

Stromversorgung

- Nennleistung: 100 – 240 V, 50 – 60 Hz
- Eingangsspannung: 90 – 264 V
- Strom: 1,5 A (RMS) bei 100 V
- Eingangsfrequenz: 47 – 63 Hz

Umgebungsbedingungen bei Betrieb

- 5 bis 35 °C
- 20 bis 80 % Luftfeuchtigkeit (nicht kondensierend)

Umgebungsbedingungen bei Nichtbetrieb

- -20 bis +60 °C
- 20 bis 80 % Luftfeuchtigkeit (nicht kondensierend)

8. Glossar

Administrator

Ein BlackArmor-Administrator ist für den BlackArmor-Server und alle seine Einstellungen verantwortlich. Administratoren können Benutzerkonten, Gruppenkonten und Freigaben erstellen oder löschen, Zugriffsberechtigungen zuweisen oder aufheben, Einstellungen des Servers ändern und weitere Administratoren einsetzen. Siehe auch Benutzer.

Arbeitsgruppe

Eine Gruppe von Computern in einem Netzwerk, die Ressourcen gemeinsam nutzen.

Archivsicherung

Siehe als Fernzugriff wird auch bezeichnet, wenn der Server über BlackArmor Manager heruntergefahren oder zurückgesetzt wird, anstatt den Netzschalter zu betätigen. Siehe auch Lokaler Zugriff.

Benutzer

In BlackArmor Manager eine Person, die den BlackArmor-Server verwenden kann, um Dateien zu speichern, zu sichern und freizugeben, die aber nicht die Berechtigung hat, Änderungen an Benutzerkonto-, Gruppenkonto-, Freigabe- oder Servereinstellungen vorzunehmen.

Benutzerkonto

Ein Konto mit einem Benutzernamen und einem Kennwort, unter dem eine Person auf den BlackArmor-Server zugreifen kann. Benutzerkonten sind mit Zugriffsberechtigungen verbunden.

CIFS

Common Internet File System (allgemeines Internet-Dateisystem). Ein Dateisystem, das die gemeinsame Nutzung von Dateien durch Benutzer mit unterschiedlichen Windows-Computern ermöglicht, ohne dass spezielle Software installiert werden muss.

Datenträger

Ein Datenspeicherbereich, der einen Teil einer Festplatte, eine ganze Festplatte oder mehrere Festplatten umfassen kann.

Domäne

Eine Gruppe von Computern, die als Einheit zentral verwaltet werden.

Ereignis

Ein Problem oder eine Änderung der Einstellungen des BlackArmor-Servers. Beispiele für Serverereignisse sind die Änderung des Servernamens oder der Ausfall einer Festplatte.

Externe USB-Festplatte

Siehe USB-Laufwerk.

Fernzugriff

Zugriff auf den Server von einem Computer, der sich nicht im lokalen Netzwerk befindet, zum Beispiel vom Computer eines Kunden über das Internet.

Als Fernzugriff wird auch bezeichnet, wenn der Server über BlackArmor Manager heruntergefahren oder zurückgesetzt wird, anstatt den Netzschalter zu betätigen. Siehe auch Lokaler Zugriff.

Firmware

Software, die fest in die Hardware integriert ist.

Formatieren

Durch Formatieren wird eine Festplatte für das Lesen und Schreiben von Daten vorbereitet. Bei der Formatierung werden Hintergrundinformationen von der Festplatte gelöscht und die Festplatte wird getestet und für den Einsatz vorbereitet. Dabei können die vorhandenen Dateien auf der Festplatte verloren gehen. Eine Festplatte muss formatiert werden, bevor sie verwendet werden kann.

Freigabe

Ein Ordner auf dem BlackArmor-Server, in dem Sicherungsdateien sowie andere Dateien, auf die andere Benutzer zugreifen können, abgelegt und geschützt werden.

FTP

File Transfer Protocol (Dateiübertragungsprotokoll). Ein Protokoll für den Austausch von Dateien über das Internet. FTP wird gewöhnlich verwendet, um Dateien über das Internet auf einen Server hochzuladen oder von einem Server herunterzuladen.

Gruppenkonto

In BlackArmor Manager eine Reihe von Benutzerkonten, die in einer Gruppe zusammengefasst werden, um den Zugriff auf Freigaben leichter verwalten zu können. Alle Benutzer einer Gruppe besitzen dieselben Zugriffsberechtigungen für die einzelnen Freigaben. Siehe auch Benutzerkonto.

Herunterfahren

In Bezug auf Festplatten: aufhören, sich zu drehen.

Hot-Swap

Austausch einer Festplatte, ohne den Server auszuschalten.

HTTP

Hypertext Transfer Protocol (Hypertext-Übertragungsprotokoll). Regeln für den Austausch der gebräuchlichsten Form von Dokumenten (Hypertext-Dokumente) über das Internet.

HTTPS

Hypertext Transfer Protocol over Secure Socket Layer (sicheres Hypertext-Übertragungsprotokoll). Regeln für den Austausch von Hypertext-Dokumenten über verschlüsselte Verbindungen.

Internet-Protokoll

Regeln für die Übertragung von Informationen über das Internet. Der BlackArmor-Server bietet zwei Internet-Protokolle zur Auswahl, HTTP und HTTPS.

IP-Adresse

Die Kennung eines Computers, Servers oder anderen Geräts in einem TCP/IP-Netzwerk. IP-Adressen bestehen aus einer Ziffernfolge, die durch Punkte gegliedert ist (z. B. 123.456.78.1). Jedes Gerät in einem lokalen Netzwerk besitzt eine eindeutige IP-Adresse.

JBOD

Just a Bunch of Drives (nur ein Haufen Festplatten). Siehe Span.

Link Aggregation

Verbindungsbündelung: Gleichzeitige Verwendung mehrerer Ethernetschnittstellen zur Verbindung mit dem Netzwerk, um eine schnellere Datenübertragung zu ermöglichen.

Wenn beide LAN-Schnittstellen des BlackArmor-Servers an den Netzwerkrouter oder Switch angeschlossen sind und in BlackArmor Manager Aggregation aktiviert ist, arbeiten beide Verbindungen gleichzeitig und parallel, sodass die Daten schneller übertragen werden – ähnlich wie wenn man einen Eimer statt mit einem mit zwei Schläuchen füllt.

Lokaler Zugriff

Zugriff auf den Server von einem Computer im lokalen Netzwerk. Oder auch manueller Zugriff auf den Server, mit physischem Kontakt zum Server oder seinen Kabeln. Siehe auch Fernzugriff.

NFS

Network File System (Netzwerkdateisystem). Ein System, mit dem alle Benutzer in einem Netzwerk Dateien gemeinsam nutzen können, die auf verschiedenen Arten von Computern gespeichert sind.

NTP-Server

Network Time Protocol Server (Netzwerkzeitprotokoll-Server). Synchronisiert Datum und Uhrzeit von Computern und Servern in einem Netzwerk auf Basis der koordinierten Weltzeit.

Parität

Bei einer RAID-5-Konfiguration werden Paritätsinformationen erzeugt, die bei Ausfall einer Festplatte im Server zur Rekonstruktion von Dateien verwendet werden. Siehe auch RAID 5.

Private Freigabe

Ein Ordner, auf den nur Benutzer zugreifen können, denen der Besitzer des Ordners die entsprechende Berechtigung erteilt hat.

RAID

Redundant Array of Independent Disks (redundante Anordnung unabhängiger Festplatten). Eine Technologie, bei der mehrere Festplatten kombiniert werden, um höhere Leistung und Ausfallsicherheit zu erzielen.

RAID 0

Siehe Stripe.

RAID 1

Siehe Spiegelung.

RAID 5

Eine RAID-Konfiguration. Bei RAID 5 werden mindestens drei Festplatten verwendet. Die Nutzung von Striping und Paritätsinformationen sorgt für Redundanz. (Paritätsinformationen dienen zur Rekonstruktion der Daten bei Ausfall einer Festplatte. Bei RAID 5 werden die Paritätsinformationen gleichmäßig auf die Festplatten mit den gespeicherten Daten verteilt.) Paritätsinformationen sorgen für Datensicherheit und Striping steigert die Leistung. Siehe auch Stripe.

RAID 10

Eine RAID-Konfiguration. Ein Datenträger mit RAID-10-Konfiguration besteht aus mehreren gleich großen RAID-1-Datenträgern. Bei RAID 10 werden sowohl Striping als auch Spiegelung verwendet. Spiegelung sorgt für Datensicherheit und Striping steigert die Leistung. Siehe auch Spiegelung und Stripe.

RSA-Schlüssel

Dient zur Entschlüsselung beim Verschlüsselungsverfahren SSL, das zum Schutz von Daten bei der Übertragung über ein Netzwerk oder das Internet verwendet wird. „RSA“ steht für Rivest, Shamir und Adelman, die Namen der Erfinder.

Seagate Global Access

Ein Service, über den Sie die Dateien auf Ihrem BlackArmor-Server von jedem Ort aus anzeigen, herunterladen, freigeben und bearbeiten können. Sie können Global Access auch nutzen, um Dateien auf Ihren BlackArmor-Server hochzuladen.

Server

Ein Computer oder Gerät in einem Netzwerk, der bzw. das Ressourcen verwaltet. Der BlackArmor-Server ist ein Dateiserver – ein Server, der zur Speicherung von Dateien dient. Er kann auch als Druckserver – ein Server, der einen oder mehrere Drucker verwaltet – verwendet werden.

SMART

Self-Monitoring Analysis and Reporting Technology (System zur Selbstüberwachung, Analyse und Statusmeldung). Eine Technologie, die in Festplatten eingebaut wird, mit der diese ihren eigenen Systemzustand überwachen und mögliche Probleme melden können. Nicht alle Festplatten verwenden SMART.

Span

Eine Gruppe von Festplatten in einem Server ohne Schutz durch RAID. Auch als „JBOD“ bezeichnet. Siehe auch RAID.

Spiegelung

Eine RAID-Konfiguration, auch als RAID 1 bezeichnet. Dabei werden auf zwei Festplatten die gleichen Daten gespeichert (gespiegelt). Im Vergleich zu unabhängigen Festplatten bietet die Spiegelung höhere Leistung, aber nur 50 % der Kapazität.

SSL-Zertifikat

Zertifikat, das bei der SSL-Verschlüsselung (Secure Socket Layer – Sockel-Sicherheitsschicht) verwendet wird. SSL (oder Transportschicht-Sicherheit) ist ein Verschlüsselungsverfahren, das zum Schutz von Daten bei der Übertragung über ein Netzwerk oder das Internet verwendet wird. Dabei wird ein System aus Schlüsseln, wie geheimen Kennwörtern, verwendet, um Dateien sicher zu versenden und zu empfangen.

Stripe

Auch als RAID 0 bezeichnet. Dabei werden die Daten in gleich großen Blöcken („stripes“ – Streifen) über mehrere Festplatten verteilt. Ein Stripesetdatenträger bietet keine Datenredundanz und damit *keine Datensicherheit*.

Die Leistung ist jedoch höher als bei einer Gruppe unabhängiger Festplatten gleicher Größe.

USB

Universal Serial Bus (universeller serieller Bus). Die Schnittstelle zwischen dem Computer und den daran angeschlossenen USB-Geräten. Der Computer kommuniziert über die USB-Schnittstelle mit den USB-Geräten.

USB-Laufwerk

Ein tragbares Laufwerk, das mit einem USB-Kabel an den Computer angeschlossen und nicht im Computer selbst installiert wird. Wird auch als Minifestplatte, Flashlaufwerk oder externe USB-Festplatte bezeichnet.

USV

Unterbrechungsfreie Stromversorgung. Eine USV ist mit einem Akku ausgestattet, um bei Stromausfällen die Stromversorgung zu einem Computer oder Server aufrechtzuerhalten. USV sind darauf ausgelegt, die Stromversorgung lange genug zu gewährleisten, um geöffnete Dateien zu speichern und das System ordnungsgemäß herunterzufahren. Sie sind nicht dazu gedacht, das System für die Dauer des Stromausfalls am Laufen zu halten.

Zugriffsstufe

Auch als Berechtigungsstufe bezeichnet. Bestimmt, in welchem Umfang ein Benutzer auf den BlackArmor®-Server zugreifen kann. In BlackArmor Manager gibt es zwei Berechtigungsstufen: *Administrator* und *Benutzer*.

Index

A

Administratoren *6*
- Einschränken des Speicherplatzes *35*
- Festlegen von Zeitlimits *49*
- Tipps für den Einstieg *12*
- Zeitlimits für die Speicherung *49*
- Zuweisen von Speicherplatz für Benutzer *35*

Administratorkennwort *16*
Aktualisieren der Firmware *46*
Anforderungen *7*
Arbeitsgruppen *44*
Automatische Firmware-Aktualisierung *46*

B

Benachrichtigungen *41*
Benutzerkonten
- Standardeinstellungen *29*

Betriebssystemunterstützung *7*
BlackArmor
- Aktualisieren der Firmware *46*
- Ausstattung *9*
- Beschreibung *8*
- Einrichtungsassistent *17*
- E-Mail-Benachrichtigungen *41*
- Energiesparen *43*
- erste Verbindung *16*
- Komponenten *9*
- LCD-Anzeige *40*
- LED-Anzeigen *40*
- Problembehebung *53*
- RAID *31*
- Sicherheit *45*
- SMART-Diagnose *41*
- Standardeinstellungen *29*
- Technische Daten *59*
- Wartung *45*
- Zurücksetzen des Servers *46*

BlackArmor Backup *9*
BlackArmor Discovery *9*
BlackArmor Manager *9*

D

Dateidienste *42*
Dateien
- Sortieren beim Herunterladen *34*

Datenträger
- RAID *31*

Discovery Tool *9*
Domänen *44*
Drag&Sort *34*
Dynamic DNS *42*

E

Einrichtungsassistent *17*
E-Mail-Benachrichtigungen *41*
Energiesparmodus *43*
Ereignisse *41*
Ethernetanschlüsse *9*

F

Festplatten *9*
- SMART-Diagnose *41*

Firmware-Aktualisierung *46*
- automatisch *46*
- manuell *46*

Freigaben
- Drag&Sort-Dienst *34*
- Einschränken des Speicherplatzes *35*
- Papierkorb-Dienst *34*
- Standardeinstellungen *29*
- Unterstützung für Dateidienste *34*
- Zeitlimits *49*

FTP *34*

G

Global Access
- aktivieren *20*
- Konto erstellen *26*

H
Herstellen der Verbindung zum Server *16*
Hilfe *7*
HTTP *44*
HTTPS *44*
I
Informationen *7*
Internet-Protokoll *44*
Internetzugriff
    Standardeinstellungen *30*
K
Klappe des Servers *10*
L
LAN-Anschlüsse *9*, *10*
LCD-Anzeige *9*, *10*, *40*
LED-Anzeigen *9*, *40*
Lieferumfang *6*
Link Aggregation *9*, *28*, *37*, *39*
M
Manuelle Firmware-Aktualisierung *46*
N
Navigationstasten der LCD-Anzeige *10*
Netzanschluss *10*
Netzschalter *10*
Netzwerk
    Standardeinstellungen *29*
NFS *34*
NTP *43*
P
Papierkorb *34*
Problembehebung *53*
R
RAID *31*
    Standardeinstellungen *29*
Reset-Taste *10*
S
SATA *9*
Schutz
    RAID *31*
Server
    Aktualisieren der Firmware *46*
    Einrichtungsassistent *17*
    E-Mail-Benachrichtigungen *41*
    Energiesparen *43*
    erste Verbindung *16*
    Festplatten *9*
    Klappe *10*
    LAN-Anschlüsse *9*, *10*
    LCD-Anzeige *9*, *10*, *40*
    LED-Anzeigen *9*, *40*
    Netzanschluss *10*
    Netzschalter *10*
    Problembehebung *53*
    RAID *31*
    Reset-Taste *10*
    Sicherheit *45*
    SMART-Diagnose *41*
    Standardeinstellungen *29*
    Systemstatus-LED *10*
    Technische Daten *59*
    USB-Anschlüsse *9*, *10*
    Wartung *45*
    Zurücksetzen *46*
Sicherheit *45*
SMART-Diagnose *41*
Sortieren von Dateien *34*
SSL *43*
Standardadministratorkennwort *16*
Standardeinstellungen
    Zurücksetzen des Servers *46*
Standardservereinstellungen *29*
Status
    E-Mail-Benachrichtigungen *41*
    LCD-Anzeige *40*
    LED-Anzeigen *40*
    SMART-Diagnose *41*
Strom *43*
Systemanforderungen *7*

Systemstatus *10*
Systemstatus-LED *10*
T
Technische Daten *59*
U
Überwachen
E-Mail-Benachrichtigungen *41*
LCD-Anzeige *40*
LED-Anzeigen *40*
Unterstützung für Dateidienste *34*
USB-Anschlüsse *9*, *10*
USV *43*
W
Wartung des Servers *45*
Z
Zeitlimits *49*
Zurücksetzen des Servers *46*